

Entanglement generation secure against general attacks

A. Pirker, V. Dunjko, W. Dür and H. J. Briegel

¹ *Institut für Theoretische Physik, Universität Innsbruck, Technikerstr. 21a, A-6020 Innsbruck, Austria*
(Dated: October 7, 2016)

We present a security proof for establishing private entanglement by means of recurrence-type entanglement distillation protocols. We consider protocols where the apparatus is imperfect, and show that nonetheless a secure quantum channel can be established, and used to e.g. perform distributed quantum computation in a secure manner. We assume an ultimately powerful eavesdropper distributing all pairs used in a subsequent distillation process by Alice and Bob, and show that even if the apparatus leaks the information about all noise processes that are realized during execution of the protocol to the eavesdropper –which arguably is the most general setting besides device independence– private entanglement is still achievable. We provide a proof of security under general quantum attacks without assuming asymptotic scenarios, by reducing such a general situation to an i.i.d. setting. Our approach relies on non-trivial properties of distillation protocols which are used in conjunction with de-Finetti and post-selection-type techniques. As a side result, we also provide entanglement distillation protocols for non-i.i.d. input states.

PACS numbers: 03.67.Dd, 03.67.Hk

Introduction.— Entanglement is a unique feature of quantum mechanics and a key resource in quantum information processing. Entanglement can be used to teleport quantum information [1], to implement remote quantum gates [2], or for distributed quantum computation [3]. It allows one to perform tasks that are not possible by classical means, such as the expansion of secret keys which can be used for secure classical communication. The latter is achieved through the famous quantum key distribution (QKD) protocols, which have been extensively studied [4–10]. In these works, security was proven in a variety of ever more general scenarios, considering noisy channels, imperfect devices and device-independent settings, where even the local quantum devices are untrusted [11–13].

In contrast, the perhaps equally important task of establishing private entanglement, and the closely related problem of establishing secure quantum channels, has not been resolved in equal generality. Secure quantum channels have only been studied in few works, under ideal settings [14, 15]. The task of establishing private entanglement has been considered in the context of noisy channels and both perfect [16] and imperfect [17, 22] local operations. However, in these works, either initial states that are identical and independently distributed (i.i.d.), or asymptotic scenarios are assumed.

In this paper we present a security proof for establishing private entanglement by means of entanglement distillation. We consider the most general attacks employed by an adversary (Eve) and assume noisy communication channels as well as noisy local operations. Specifically, the eavesdropper distributes the ensemble of Bell-pairs to Alice and Bob subject to entanglement distillation. Moreover, we assume that the noisy apparatus may leak all the information about the noise processes which have occurred in a run of the protocol to Eve. This is arguably the most general scenario which can be considered for

protocols with a quantum output, as strong device independence can only be enforced for protocols where the outputs are classical [32]. We first provide a security analysis for i.i.d. inputs and we show how to generalize these results to non-i.i.d. states. This is done by employing de-Finetti and post-selection techniques. We note, however, that these techniques cannot be straightforwardly applied, but need to be adapted and modified to be applicable. We present and discuss the required additional steps of preprocessing, and provide entanglement distillation protocols that are not restricted to i.i.d. input states, but are capable of dealing with general (correlated) inputs. The latter is related to recent results in [18–20].

The model and security guarantees.— Entanglement distillation is modelled by considering three players, Alice and Bob, who wish to generate a shared Bell pair, and Eve, who provides the initial pairs. Thus, Eve is connected to Alice and to Bob via a (generally noisy) quantum channel which may be completely under her control. Alice and Bob are connected by a classical authenticated, but not necessarily confidential, channel. Distillation protocols assume that Alice and Bob apply local, in general noisy, quantum operations to their pairs. To model this noise, we employ and extend the approach of [17], where a noise register, referred to as the “lab demon” (L) register L used to store classical information about the local noise history with the help of classical flags, is appended to Alice and Bob’s pairs. In this work, we model those flags by quantum registers, attached to Alice and Bob. We represent the noisy maps of the distillation process as unitaries acting on an enlarged Hilbert space. L thereby coherently applies Pauli operators onto the registers of Alice and Bob which is equivalent to local depolarizing noise. Due to the symmetry of Bell states $|B_{00}\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$, it suffices to consider the case when the noise is applied on, say, Alice’s register only. To model the setting where

Eve acquires information about the noise transcript during the execution of the protocol, we simply assume that L informs Eve which noise operator was applied at each step. The overall set-up is given in Fig. 1. In the remainder of this paper we elaborate further on the full quantum treatment of L and Eve in terms of purifications which goes beyond the problem setting introduced in [17].

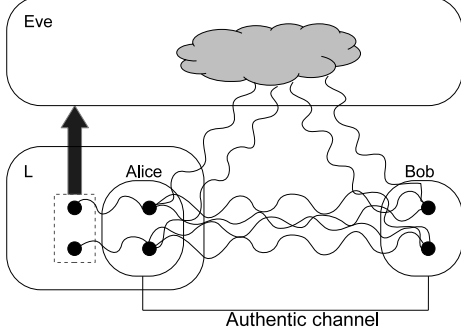


FIG. 1. Illustration of the overall setting: Eve provides the initial pairs to Alice and Bob, who run the distillation protocol. The noisy apparatus may leak the specification of the realized noise map to Eve after every step of the protocol.

The proposed overall protocol under i.i.d. assumption involves several steps. First, Eve distributes n pairs, also referred to as initial states, to Alice and Bob who apply local “twirl” operations (employing random, correlated local operations). Next, Alice and Bob sacrifice some $m \approx \sqrt{n}$ pairs to check whether the fidelity, defined as $F(\rho, \sigma) = \text{tr} \sqrt{\rho^{1/2} \sigma \rho^{1/2}}$ for density operators ρ and σ , of the pairs is sufficiently high for distillation, via local σ_x and σ_z measurements. If the fidelity F relative to $|B_{00}\rangle$ is too small they abort the procedure. Otherwise they proceed with a recurrence-type entanglement distillation to produce a high fidelity Bell-pair from the remaining initial states, which may also be aborted. Finally, Alice and Bob output their final state. The purpose of each of these steps is clear in the case of i.i.d. inputs. For instance, in the i.i.d. case, the twirl ensures that local σ_z and σ_x correlation measurements can be used to estimate the fidelity of individual pairs. Later, we will generalize to non-i.i.d. settings and the protocol be prepended by symmetrization (permuting of the pairs) and tracing-out steps.

To formalize the security requirements, we define the ideal map $\mathcal{F}^{\alpha, l}$, mapping the initial states of Alice and Bob to a single Bell-pair, where α (abstractly) characterizes the noise levels in the channels connecting Eve to Alice and Bob, and also the noise of the local devices. The ideal map can intuitively be thought of as a map which simulates a real protocol as follows. In the case of an abort, it outputs whatever final state was reached. In the non-aborting case, however, it replaces the actual output with a special state $\sigma_{ABE}^{\alpha, \mathcal{P}, l}$, which corresponds to

the output of a real protocol, utilizing distillation protocol \mathcal{P} , that was successfully run with asymptotically many high-fidelity i.i.d. initial pairs. This is the best the noisy distillation protocol \mathcal{P} could ever do. As we show later, $\sigma_{ABE}^{\alpha, \mathcal{P}, l}$ is a well-defined state for the distillation protocols and noise parameters considered here, that is, it depends on the local noise parameters *only* and not the initial states. Formally, we have:

$$(\mathcal{F}^{\alpha, l} \otimes id_E)(|\psi\rangle\langle\psi|_{ABE}) = p_\rho \sigma_{ABE}^{\alpha, \mathcal{P}, l} \otimes |ok\rangle\langle ok|_f + (1 - p_\rho) \sigma_{ABE}^\perp \otimes |fail\rangle\langle fail|_f \quad (1)$$

where $|\psi\rangle_{ABE}$ is a purification of the initial n -partite ensemble $\rho_{AB}^{(n)}$ provided by Eve, p_ρ is the success probability depending on the input state $\rho_{AB}^{(n)}$, and σ_{ABE}^\perp is some fixed state output if the protocol is aborted. The two-level flag system f distinguishes the accepting from the aborting branch. The state $\sigma_{ABE}^{\alpha, \mathcal{P}, l}$ is the asymptotic state of the distillation protocol \mathcal{P} and is of the form

$$\sigma_{ABE}^{\alpha, \mathcal{P}, l} = \left(\sum_{i,j=0}^1 \omega_{ij}(\alpha, \mathcal{P}) |B_{ij}\rangle\langle B_{ij}|_{AB} |\eta_{ij}\rangle\langle\eta_{ij}|_E \right) \otimes \sigma_E \quad (2)$$

where $|\eta_{ij}\rangle$ are the leaked noise transcript of Eve, $|B_{ij}\rangle = (id \otimes \sigma_x^j \sigma_z^i) |B_{00}\rangle$ the Bell-basis states, and $\omega_{ij}(\alpha, \mathcal{P})$ are probabilities which depend on the noise level of the local devices and the distillation protocol \mathcal{P} . For instance, if the local devices are perfect then $\omega_{ij} = 1$ if and only if $i = j = 0$, hence AB contains a perfect Bell-pair. Finally, the states $|\eta_{ij}\rangle$ contain the sequences of noise operations, and are orthogonal for different i, j . If the noise transcripts do not leak to Eve, we denote the ideal protocol by \mathcal{F}^α . In that case, $|\eta_{ij}\rangle$ in (2) is not accessible to Eve, hence we replace $\sigma_{ABE}^{\alpha, \mathcal{P}, l}$ by $\sigma_{ABE}^{\alpha, \mathcal{P}} = \left(\sum_{i,j} \omega_{ij}(\alpha, \mathcal{P}) |B_{ij}\rangle\langle B_{ij}|_{AB} \right) \otimes \sigma_E$ in (1).

In the following we define the 1-norm of a density operator ρ by $\|\rho\|_1 = \text{tr} \sqrt{\rho \rho^\dagger}$. A distillation protocol (together with the noise maps), given as a CPTP map $\mathcal{E}^{\alpha, (l)}$, is confidential if it is close to the ideal map:

Definition 1. The protocol $\mathcal{E}^{\alpha, (l)}$ is ε -confidential, if

$$\|(\mathcal{E}^{\alpha, (l)} \otimes id_E - \mathcal{F}^{\alpha, (l)} \otimes id_E)(|\psi\rangle\langle\psi|_{ABE})\|_1 \leq \varepsilon \quad (3)$$

holds for all initial states $|\psi\rangle_{ABE}$.

In this definition, the system E may contain any purification of the initial states Eve provided. The classical communication is not correlated to the output of the real protocol, thus it can be ignored, see [23] for details. The robustness of the protocol [33] is considered in [23].

We outline the rest of the paper as follows: First we establish necessary conditions to guarantee confidentiality for recurrence-type distillation protocols restricted to

i.i.d. inputs whenever the noise transcripts do not leak to Eve. Then we generalize those conditions to arbitrary initial states via the de-Finetti theorem [24]. Next we use them to prove the confidentiality criterion (3) for distillation protocols where the noise transcripts do not leak. Finally, this will imply the confidentiality bound for distillation protocols whenever the noise transcripts of L leak to Eve.

Entanglement distillation for i.i.d. inputs.— The basic step of a recurrence-type distillation protocol can be summarized as follows: Alice and Bob share two noisy Bell-pairs, that is both have two qubits, each representing a "half" of a noisy Bell pair, and they first apply local operations to their respective parts of two Bell-pairs; next, they measure one Bell-pair and classically communicate their respective outcomes. Depending on the distillation protocol and the observed outcomes they either keep or discard the unmeasured pair. The basic step is applied to all pairs of the initial states, which comprises one distillation round. This distillation round is iterated where output states of the previous round are used as inputs for the next round. In the limit, a noiseless distillation protocol outputs a perfect Bell-pair which implies that Eve is factored out.

For the BBPSSW protocol [28] it has been shown analytically in [27] that for local imperfect operations, where the noise is assumed to be local depolarizing, there exists a unique and attracting fixed point of the protocol which only depends on the noise parameters. In other words, whenever the fidelity of the initial states relative to $|B_{00}\rangle$ is above some minimum fidelity F_{\min} , depending on the noise parameters, the protocol converges towards that unique fixed point. We find that the output state σ_{AB}^N , where $N = \log_2 n$ denotes the number of successful completed layers of distillation, satisfies $\|\sigma_{AB}^N - \sigma_{AB}^{\alpha;B}\|_1 \leq \varepsilon_B$, where ε_B is naturally a function of N , and it holds that $\varepsilon_B \leq F(n) \in O(n^{-b_B(\alpha)})$ and $0 < b_B(\alpha) \leq \log_2 3 - 1$.

For the distillation protocol of Deutsch et. al. [16] (referred to as the DEJMPS protocol) the fixed point analysis turns out to be more complicated. In the noiseless case, DEJMPS was proven to have a unique attracting fixed point [21]. For the noisy case we can only provide extensive numerical evidence that there exists a unique and attracting fixed point depending on the noise parameters only, see [23]. We numerically find that for the state σ_{AB}^N obtained after successfully completing $N = \log_2 n$ layers of distillation that $\|\sigma_{AB}^N - \sigma_{AB}^{\alpha;D}\|_1 \leq \varepsilon_D$ where ε_D is naturally a function of N , and it holds that $\varepsilon_D \leq F(n) \in O(n^{-b_D(\alpha)})$. $b_D(\alpha)$ is a strictly positive function.

Since in the abort case the outputs of the overall protocol \mathcal{E}^α and the ideal protocol \mathcal{F}^α are identical, we obtain for both protocols that

$$\|(\mathcal{E}^\alpha - \mathcal{F}^\alpha)(\rho_{AB}^{\otimes n})\|_1 \leq \varepsilon, \quad (4)$$

where $\varepsilon = \varepsilon_B$ for the BBPSSW and $\varepsilon = \varepsilon_D$ for the DE-

JMPS protocol for all i.i.d. inputs $\rho_{AB}^{\otimes n}$. Hence, in both cases, the final distance to the respective fixed points scales polynomial in terms of initial states.

The functions $b_B(\alpha)$ and $b_D(\alpha)$ of the local noise level α thus govern the rate of convergence of the real protocol to the ideal protocol in the i.i.d. case for distillation protocols. We numerically found that these functions monotonically grow as the local noise rate α tends to zero [23]. Thus increasing the fidelity of local devices (through e.g. fault-tolerance) directly influences the rate of convergence, which in turn governs the security level. In contrast to $b_B(\alpha)$, the function $b_D(\alpha)$ is not upper bounded which implies that for certain noise parameters α the DEJMPS protocol needs to perform less distillation rounds than the BBPSSW protocol to achieve the required confidentiality of Alice and Bob.

Now we use the established results regarding the fixed point properties of distillation protocols for i.i.d. initial states to show that similar results hold for arbitrary initial states.

Entanglement distillation for arbitrary inputs.— In generalizing the previous results to arbitrary initial states we make use of the de Finetti theorem [24]. The basic de-Finetti results guarantee that the reduced state $\text{tr}_{n-k}(\rho_{AB}^{(n)})$ of a permutation symmetric n -partite state $\rho_{AB}^{(n)}$ is close to an i.i.d. state $\int \sigma_{AB}^{\otimes k} d\sigma$, with distance which scales as $O(k/n)$. Thus we have for the prepended protocols $\mathcal{E}^{s\&t}$ and $\mathcal{F}^{s\&t}$ for arbitrary initial states ρ_{AB} that

$$\begin{aligned} \|\mathcal{E}^{s\&t}(\rho_{AB}) - \mathcal{F}^{s\&t}(\rho_{AB})\| \\ \leq 64k/n + \max_{\sigma_{AB}} \|(\mathcal{E} - \mathcal{F})(\sigma_{AB}^{\otimes k})\|_1 \end{aligned} \quad (5)$$

where symmetrization (denoted by s) is followed by tracing out $n-k$ subsystems (denoted by t) via the de Finetti theorem. In (5) we have omitted the superscript α characterizing the noise level, and we shall omit it from now on, unless it is specifically needed. Inequality (5) implies that the properties of the fixed point (unique, attracting, noise-dependence) also hold for arbitrary initial states if the protocol is prepended by symmetrization and trace out. This enables us to prove the confidentiality criterion of Definition 1 for distillation protocols where the noise transcripts of L do not leak to Eve, which in turn will finally imply the confidentiality criterion (3) whenever the noise transcripts do leak.

Confidentiality of distillation protocols.— The inequality in (4) establishes the local properties of the protocol, and is more or less typical for studies in the context of the convergence of distillation protocols in the i.i.d. case. However it falls short of the complete characterization captured by the confidentiality criterion (3) in two ways: first, the input states are restricted (i.i.d.); second, it fails to consider the purifying system of Eve [34], vital in cryptographic contexts. While the prior issue is the subject of

de-Finetti and post-selection-type reductions, the latter issue can be a problem in general, small distance of corresponding subsystems does not imply a small distance of the total systems.

However, we can resolve this issue by using the fixed point properties of distillation protocols for arbitrary initial states. More precisely, we relate the two distances by the following Lemma, proven in [23].

Lemma 2. *Let \mathcal{E} be the real distillation protocol which is guaranteed to converge towards a unique, attracting fixed point depending on the noise parameters only in the ok-branch. Furthermore let \mathcal{F} be the ideal protocol as defined previously. Then*

$$\max_{\rho_{AB}} \|\mathcal{E}(\rho_{AB}) - \mathcal{F}(\rho_{AB})\|_1 \leq \varepsilon, \text{ implies that} \quad (6)$$

$$\|(\mathcal{E} \otimes id_E - \mathcal{F} \otimes id_E)(|\psi\rangle\langle\psi|_{ABE})\|_1 \leq C\varepsilon$$

for all $|\psi\rangle_{ABE}$ where $C = 2^{14} + 1$.

Lemma 2 is vital as it allows us to easily employ the de-Finetti theorem [24]. Hence, for the protocols $\mathcal{E}^{s\&t}$ and $\mathcal{F}^{s\&t}$ we obtain by using the de Finetti theorem in conjunction with Lemma 2:

$$\max_{|\psi\rangle_{ABE}} \|(\mathcal{E}^{s\&t} \otimes id_E - \mathcal{F}^{s\&t} \otimes id_E)(|\psi\rangle\langle\psi|)\|_1 \leq \varepsilon', \quad (7)$$

where $\varepsilon' = (2^{14} + 1)(64k/n + \max_{\sigma_{AB}} \|(\mathcal{E} - \mathcal{F})(\sigma_{AB}^{\otimes k})\|_1)$. Thus, arbitrary security levels can be reached, however at the cost of wasting some pairs, and the scaling is linear. If the local noise is low, we can do better in terms of scaling and efficiency, using the post-selection technique [8]. For that purpose we first establish a similar result to (6) by using the fact that the final state after the protocol including L is pure.

Lemma 3. *Let \mathcal{E} be the real protocol and \mathcal{F} be the ideal protocol satisfying the assumptions of Lemma 2. Then given any state $\rho_{AB}^{(n)}$ we have that*

$$\|\mathcal{E}_L(\rho_{AB}^{(n)}) - \mathcal{F}_L(\rho_{AB}^{(n)})\|_1 \leq \varepsilon, \text{ implies that} \quad (8)$$

$$\|(\mathcal{E} \otimes id_E - \mathcal{F} \otimes id_E)(|\psi\rangle\langle\psi|_{ABE})\|_1 \leq 4\sqrt{\varepsilon}$$

for all purifications $|\psi\rangle\langle\psi|_{ABE}$ of $\rho_{AB}^{(n)}$ where \mathcal{E}_L and \mathcal{F}_L denote the extensions of the distillation protocol to L.

The Lemma mainly relies on the unitary equivalence of purifications and the purity of the final state including L. For the complete proof of Lemma 3 we refer the reader to [23].

The post-selection technique is applicable to protocols which include a symmetrization step. In our case, this technique establishes that if the protocol satisfies the confidentiality criterion (3) (within ε), for one specific initial state $\tau_{ABE'}$, the so-called purified de-Finetti state

($\tau_{ABE'}$ is any state purifying $\int \sigma_{AB}^{\otimes n} d\sigma$, which itself is a randomly chosen i.i.d. state under a certain measure), then it satisfies the same inequality for any initial state, within $\varepsilon' \leq \varepsilon(n+1)^{15}$. Recall, here n is the number of initial states (noisy Bell-pairs). By combining the post-selection technique [8] with Lemma 3, we have for the real and ideal protocol with initial symmetrization (\mathcal{E}^s and \mathcal{F}^s), and all initial states $|\psi\rangle_{ABE}$, that

$$\|(\mathcal{E}^s \otimes id_E - \mathcal{F}^s \otimes id_E)(|\psi\rangle\langle\psi|)\|_1 \leq 4\varepsilon(n+1)^{15}, \quad (9)$$

where $\varepsilon = \max_{\sigma_{AB}} \sqrt{\|(\mathcal{E} - \mathcal{F})(\sigma_{AB}^{\otimes n})\|_1}$. As we have clarified earlier, the scaling of ε as a function of n depends on the noise parameters, hence the bound ε' on the total confidentiality level scales as $O(n^{15-b(\alpha)/2})$. Of particular importance is the value for the noise level α at which $b(\alpha) > 30$, as this is the threshold at which the post-selection-based reduction becomes feasible. We find that this value is achieved at extremely low noise rates α_{bound} . Notice that the de-Finetti theorem allows to proof confidentiality also for higher error rates. For the simplified setting of binary pairs numerical computations suggest for the DEJMPS protocol $\alpha_{bound} \approx 10^{-19}$, see [23]. In contrast, the post-selection technique is not applicable to the BBPSSW protocol at all due to its slow and bounded rate of convergence. While such rates are unlikely to be achievable on the physical level, they are, at least in principle, possible through fault-tolerant constructions.

We conclude that recurrence-type distillation protocols prepended by a symmetrization and a system discarding step are confidential according to Definition 1 by Eq. (7) for all noise levels α for which distillation is possible in the i.i.d. case. This implies that the final state in the ok-branch is close to a tensor product state, i.e. Eve is factored out. The obtained results regarding the BBPSSW protocol are analytic whereas for the DEJMPS protocol the results rely on strong numerical evidence. For low noise rates, distillation protocols are confidential according to Eq. (9).

Confidentiality of distillation protocols whenever the noise transcripts leak.— Finally we provide security guarantees for distillation protocols assuming that the noise transcripts leak to Eve, i.e. the most general setting besides device-independence. For that purpose we relate the confidentiality criterion (3) for protocols where the noise transcripts leak to Eve to the previously established results. More formally, we have the following Lemma.

Lemma 4. *Let \mathcal{E} be the real protocol and \mathcal{F} be the ideal protocol satisfying the assumptions of Lemma 2. Furthermore, let \mathcal{E}^l denote the real and \mathcal{F}^l the ideal protocol when the noise transcripts leak to Eve. Then*

$$\|(\mathcal{E} \otimes id_E - \mathcal{F} \otimes id_E)(|\psi\rangle\langle\psi|)\| \leq \varepsilon, \text{ implies} \quad (10)$$

$$\|(\mathcal{E}^l \otimes id_E - \mathcal{F}^l \otimes id_E)(|\psi\rangle\langle\psi|)\| \leq 2\sqrt{\varepsilon}$$

for all $|\psi\rangle_{ABE}$.

The proof, see [23], uses the unitary equivalence of purifications. Lemma 4 establishes via (10) that if a distillation protocol is ε -confidential according to Definition 1 then the protocol is $2\sqrt{\varepsilon}$ -confidential if the noisy apparatus leaks the noise transcripts to Eve.

Discussion.— We have shown that recurrence-type entanglement distillation protocols lead to private entanglement without referring to the asymptotic limit. This holds true even when the local devices are noisy, and when the potential eavesdropper is able to completely monitor the operation of these devices in run-time (i.e., the noisy apparatus leaks information about the realized noise processes) in which case she is classically correlated to Alice and Bob at the very end. Furthermore, if the noise transcripts do not leak, she is even in tensor product with Alice and Bob, i.e. “factored out”. Our protocol can, for instance, be used to realize private quantum channels by means of teleportation - the only information that may leak to Eve after teleportation is which noise map was applied to the sent state, but nothing about the state itself (see [23] for details). Our definitions also imply the security of the protocol in arbitrary settings (beyond the application to quantum channels), thus this opens the way for the secure realization of various quantum task: it can be used to establish quantum channels and quantum networks, for applications such as distributed quantum computation. Aside from cryptographic aspects, the proposed protocol can be used to generate high quality entanglement from sources which are not guaranteed to produce i.i.d. states.

We acknowledge the support by the Austrian Science Fund (FWF) through the SFB FoQuS F 4012 and projects P24273-N16, P28000-N27. AP and VD are grateful to Christopher Portmann for useful discussions, comments, and advice concerning technical aspects of this work.

-
- [1] Bennett, C. H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., Wootters, W. K., Phys. Rev. Lett. 70, 1895 (1993).
 - [2] Bennett, C. H., DiVincenzo, D. P., Shor, P. W., Smolin, J. A., Terhal, B. M., Wootters, W. K., Phys. Rev. Lett., 87, 077902 (2001).
 - [3] Cirac, J. I., Ekert, A. K., Huelga, S. F., Macchiavello, C., Phys. Rev. A 59, 4249 (1999).
 - [4] Lo, H. K., A simple proof of the unconditional security of quantum key distribution, Journal of Physics A: Mathematical and General 34(35), 6957 (2001).
 - [5] Gottesman, D., Lo, H. K., Proof of security of quantum key distribution with two-way classical communications, Information Theory IEEE Transactions on 49(2), 457-475 (2003).
 - [6] Shor, P. W., Preskill, J., Phys. Rev. Lett. 85, 441 (2000).
 - [7] Baigneres, T., Quantum Cryptography: On the Security of the BB84 Key-Exchange Protocol, No. LASEC-STUDENT-2006-001 (2003).
 - [8] Christandl, M., König, R., Renner, R., Phys. Rev. Lett. 102, 020504 (2009).
 - [9] Renner, R., Security of quantum key distribution, International Journal of Quantum Information 6.01, 1-127 (2008).
 - [10] Zhao, Y. B., Yin, Z. Q., Apply current exponential de Finetti theorem to realistic quantum key distribution, In International Journal of Modern Physics: Conference Series Vol. 33, 1460370 (2014).
 - [11] Acin, A., Brunner, N., Gisin, N., Massar, S., Pironio, S., Scarani, V., Phys. Rev. Lett. 98, 230501 (2007).
 - [12] Lim, C. C. W., Portmann, C., Tomamichel, M., Renner, R., Gisin, N., Phys. Rev. X, 3, 031006 (2013).
 - [13] Vazirani, U., Vidick, T., Phys. Rev. Lett. 113, 140501 (2014).
 - [14] Barnum, H., Crépeau, C., Gottesman, D., Smith, A., Tapp, A., Authentication of quantum messages, In Foundations of Computer Science, Proceedings, The 43rd Annual IEEE Symposium, 449-458, (2002)
 - [15] Hayden, P., Leung D., Mayers D., *Authentication of quantum messages*. Applications of Lasers for Sensing and Free Space Communications. Optical Society of America (2011).
 - [16] Deutsch, D., Ekert, A., Jozsa, R., Macchiavello, C., Popescu, S., Sanpera, A., Phys. Rev. Lett. 77, 2818 (1996).
 - [17] Aschauer, H., Briegel, H. J., Phys. Rev. Lett. 88, 047902 (2002).
 - [18] Brandão, F. G., Eisert J., Correlated entanglement distillation and the structure of the set of undistillable states, Journal of Mathematical Physics 49.4, 042102 (2008).
 - [19] Buscemi, F., Datta N., Distilling entanglement from arbitrary resources, Journal of Mathematical Physics 51.10, 102201 (2010).
 - [20] Waeldechen, S., Gertis, J., Campbell, E. T., Eisert, J., Phys. Rev. Lett. 116, 020502 (2016).
 - [21] Macchiavello, C., Phys. Lett. A 246, 385-388 (1998)
 - [22] Aschauer, H., Briegel, H. J., Phys. Rev. A. 66, 032302 (2002).
 - [23] The supplementary material.
 - [24] Christandl, M., König, R., Mitchison, G., Renner, R., One-and-a-half quantum de Finetti theorems, Communications in Mathematical Physics 273(2), 473-498 (2007).
 - [25] Hoeffding, W., Probability inequalities for sums of bounded random variables, Journal of the American statistical association 58.301, 13-30 (1963).
 - [26] Serfling, R. J., Probability inequalities for the sum in sampling without replacement, The Annals of Statistics, 39-48 (1974).
 - [27] Dür, W., Briegel, H. J., Cirac, J. I., Zoller, P., Phys. Rev. A 59, 169-181 (1999).
 - [28] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, W. K. Wootters, Phys. Rev. Lett. 76, 722 (1996).
 - [29] Nielsen, M. A., Chuang, I.L., Quantum computation and quantum information, Cambridge university press (2010).
 - [30] Dür, W., Briegel, H. J., Entanglement purification and quantum error correction, Reports on Progress in Physics 70.8, 1381 (2007).
 - [31] Altepeter, J. B., Jeffrey, E. R., Kwiat, P. G., Photonic state tomography. Advances in Atomic, Molecular, and

Optical Physics 52, 105-159 (2005).

- [32] Observe that in device independent settings one assumes that honest players only have classical access to uncharacterized devices. By allowing quantum output, independent of the protocol, unpreventable malicious tampering can always occur.
- [33] The robustness is quantified by the abort probability in the all-honest, but noisy setting.
- [34] Technically, inequality (4) is a statement about the operator norm-induced distance on maps, where expression of (3) is the completely bounded diamond norm, relevant for security statement.

Entanglement generation secure against general attacks - Supplemental Material

The supplemental material is organized as follows: We first consider entanglement distillation protocols for i.i.d. inputs. For that purpose we start with the DEJMPS protocol [16] followed by the BBPSSW protocol [28]. Next we use the results obtained for i.i.d. inputs to provide confidentiality guarantees for arbitrary input states. More precisely, the fixed point properties of the respective protocols will enable us to derive confidentiality bounds. This will imply in the next section the confidentiality of the respective protocols whenever the noise transcripts leak to Eve. Furthermore we provide an analysis if the final state of the entanglement distillation protocol is quantum one-time padded as this immediately decouples Eve, i.e. the state after quantum one-time padding is separable with respect to Alice/Bob and Eve. To complete the security characterization of the proposed protocols, we introduce the robustness of entanglement distillation protocols. Finally we show how our proposed protocols can be used to establish secure quantum channels by means of quantum teleportation.

ENTANGLEMENT DISTILLATION FOR I.I.D. INPUTS

The DEJMPS protocol

We first provide an overview of the DEJMPS protocol [16] and then extend the description incrementally to our proposed setting (including L and Eve).

The DEJMPS protocol is a recurrence-type entanglement distillation protocol which combines several noisy copies of a mixed state ρ to distill a state arbitrarily close to the maximally entangled state $|B_{00}\rangle$, where $|B_{ij}\rangle = (id \otimes \sigma_x^j \sigma_z^i)(|00\rangle + |11\rangle)/\sqrt{2}$ for $i \in \{0, 1\}$ and $j \in \{0, 1\}$, provided that the fidelity $F = \langle B_{00} | \rho | B_{00} \rangle$ satisfies $F > 1/2$ for the noiseless case. If the apparatus is noisy, then the minimal required fidelity F needs to satisfy $F > F_{min}$ (where F_{min} depends on the noise level of the apparatus) to achieve distillation. For more details on recurrence-type distillation protocols in general we refer the interested reader to [30]. A basic step of the DEJMPS protocol is as follows:

Protocol 1: Basic step of the DEJMPS protocol

Require: Input state of Alice and Bob: $\rho^{(a_1, b_1)} \otimes \rho^{(a_2, b_2)}$

1: Alice and Bob apply the local basis change $U_x = e^{-i\pi/4\sigma_x^{(a_1)}} \otimes e^{i\pi/4\sigma_x^{(b_1)}} \otimes e^{-i\pi/4\sigma_x^{(a_2)}} \otimes e^{i\pi/4\sigma_x^{(b_2)}}$:

$$U_x \left(\rho^{(a_1, b_1)} \otimes \rho^{(a_2, b_2)} \right) U_x^\dagger.$$

2: Alice and Bob apply a bilateral CNOT (BCNOT):

$$(\text{CNOT}_{a_1 \rightarrow a_2} \otimes \text{CNOT}_{b_1 \rightarrow b_2}) \rho^{(a_1, b_1)} \otimes \rho^{(a_2, b_2)} (\text{CNOT}_{a_1 \rightarrow a_2} \otimes \text{CNOT}_{b_1 \rightarrow b_2})^\dagger.$$

3: Alice and Bob apply a $\sigma_z^{(a_2)} = \sigma_z \otimes id$ and a $\sigma_z^{(b_2)} = id \otimes \sigma_z$ measurement

4: Alice and Bob communicate their measurement outcomes, z_a and z_b respectively, over a classical authentic channel

5: **if** $z_a = z_b$ **then**

6: Alice and Bob keep the subsystems a_1 and b_1 of step 2

7: Alice and Bob discard the measured subsystems a_2 and b_2

8: **else**

9: Alice and Bob discard both pairs

10: **end if**

Hence, we can write one basic distillation step of the DEJMPS protocol as the linear map $O_{2\text{-EPP}}(\rho \otimes \rho) = O'_{2\text{-EPP}}(\rho \otimes \rho) O_{2\text{-EPP}}^\dagger$ where

$$O'_{2\text{-EPP}} = \left(id_{a_1, b_1} \otimes P_z^{(a_2)} \otimes P_z^{(b_2)} \right) (\text{CNOT}_{a_1 \rightarrow a_2} \otimes \text{CNOT}_{b_1 \rightarrow b_2}) U_x$$

modulo a normalization factor and where $P_z = |z\rangle\langle z|$, $z \in \{0, 1\}$ denotes the respective outcome of step 3 of Protocol 1.

The basic step is applied to all initial pairs, which comprises one distillation round. This distillation round is iterated where output states of the previous round are used as inputs for the next round. So we summarize the DEJMPS protocol as follows:

Protocol 2: DEJMPS protocol

Require: Input state of Alice and Bob: $\bigotimes_{i=1}^{2^n} \rho^{(a_i, b_i)}$ where $F = \langle B_{00} | \rho^{(a_i, b_i)} | B_{00} \rangle > 1/2$ for all $i \in \{1, \dots, 2^n\}$

- 1: **while** Pairs left for distillation **do**
- 2: Apply Protocol 1 to all pairs
- 3: Use the outputs of the previous step as input for the next distillation round
- 4: **end while**

We remind the reader that the recurrence relations of the protocol (i.e. update functions of the coefficients of an ensemble) are central for the convergence analysis of the DEJMPS protocol. For Bell-diagonal states, i.e. states of the form

$$\rho = p_{00} |B_{00}\rangle \langle B_{00}| + p_{11} |B_{11}\rangle \langle B_{11}| + p_{01} |B_{01}\rangle \langle B_{01}| + p_{10} |B_{10}\rangle \langle B_{10}|$$

where $\sum_{ij} p_{ij} = 1$, $p_{ij} \geq 0$, a straightforward computation yields the recurrence relations for the DEJMPS protocol to be

$$\begin{aligned} \tilde{p}_{00} &= \frac{p_{00}^2 + p_{11}^2}{N}, & \tilde{p}_{11} &= \frac{2p_{01}p_{10}}{N}, \\ \tilde{p}_{01} &= \frac{p_{01}^2 + p_{10}^2}{N}, & \tilde{p}_{10} &= \frac{2p_{00}p_{11}}{N} \end{aligned} \quad (11)$$

where $N = (p_{00} + p_{11})^2 + (p_{01} + p_{10})^2$, see e.g. [16].

In [21] it has been shown analytically that the recurrence relations (11) converge towards a unique and attracting fixed point provided the initial fidelity with $|B_{00}\rangle$, p_{00} , is above $1/2$.

The recurrence relations of the DEJMPS protocol taking independent single qubit white noise, i.e. noise of the form $N\rho = f\rho + (1-f)/4(\rho + \sigma_x\rho\sigma_x + \sigma_y\rho\sigma_y + \sigma_z\rho\sigma_z)$ acting on each qubit of Alice into account, read far more complex. In the presence of noise we have strong numerical evidence that the DEJMPS protocol converges towards a unique and attracting fixed point depending on the noise level f only.

From figure 2 we suggest a linear relationship between $\log \|\rho_{\text{fix}} - \rho_n\|_1$ (where ρ_{fix} and ρ_n denote the fixed point and the state after successfully completing n distillation rounds respectively) and the number of successful distillation rounds n . We immediately observe that the slope only depends on the noise parameter f , i.e. we have that

$$\log \|\rho_{\text{fix}} - \rho_n\|_1 = a(f) - nb(f).$$

Using $\log_2 N = n$, where N denotes the number of input pairs, this implies $\|\rho_{\text{fix}} - \rho_n\|_1 = e^{a(f)} e^{-b(f) \log_2 N} = a'(f) N^{-b'(f)}$, i.e. $\|\rho_{\text{fix}} - \rho_n\|_1$ scales as $F(N) \in O(N^{-b'(f)})$ as mentioned in the main text. Furthermore we numerically find that the function $b'(f)$ monotonically grows for $f \rightarrow 1$.

Detailed analysis including L

We outline the remainder of this section as follows: First we derive the recurrence relations of the DEJMPS protocol in the most general setting, taking the noise applied by L into account as well as assuming that Eve receives the leaked noise transcripts of L. We use those recurrence relations in the next subsection to provide analytical results regarding the fixed point of the recurrence relations, where the inputs are binary pairs and L only applies either id or σ_x operators. We close the section with numerical results for general i.i.d. Bell-diagonal pairs and the most general noise maps of L.

The recurrence relations

For i.i.d. input states the state of each system subject to distillation at an intermediate distillation round of the

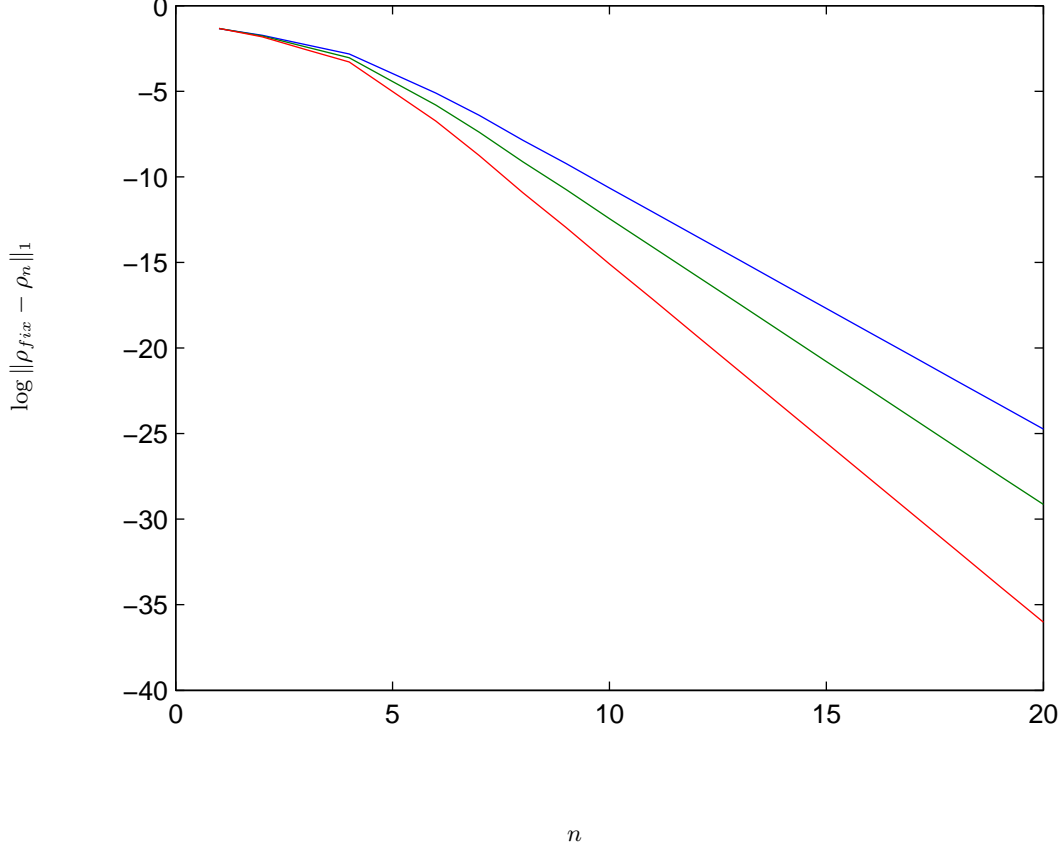


FIG. 2. The figure illustrates $\log \|\rho_{\text{fix}} - \rho_n\|_1$ for different noise parameters $f = 0.97$ (blue), $f = 0.98$ (green) and $f = 0.99$ (red). The fixed point ρ_{fix} was evaluated for 500 iterations of the DEJMPS protocol.

DEJMPS protocol is of the form $|\Psi\rangle_{ABEL} = \sum_{i,j,k,l} P_{ijkl} |B_{ij}\rangle_{AB} |kl\rangle_L |ijkl\rangle_E$, where P_{ijkl} are probability amplitudes, if we assume the noise is leaked to Eve after every distillation round. The system AB models the pair of Alice and Bob, L the system of L (where the content of the register corresponds to the effective noise introduced to AB) and E the system of Eve. L applies the noise processes before a basic protocol step to the systems of Alice. Moreover, L keeps track of the effective noise introduced using its system in a sense we clarify later.

In the following we use the notation

$$\sigma_{0,0} = id, \quad \sigma_{0,1} = \sigma_x, \quad \sigma_{1,0} = \sigma_z, \quad \sigma_{1,1} = \sigma_y$$

for the four Pauli-operators. Furthermore we denote by superscripts in brackets particle labels and by superscripts without brackets the power of an operator.

L introduces the noise maps $U_{\alpha_1, \beta_1, \alpha_2, \beta_2} = U_{\alpha_1, \beta_1}^{(a_1)} \otimes U_{\alpha_2, \beta_2}^{(a_2)}$ where $U_{\alpha, \beta}^{(a_k)} = \sigma_{\alpha, \beta}^{(a_k)} \otimes ((\sigma_x^\alpha) \otimes (\sigma_x^\beta))^{(L_k)}$. We observe that applying the noise map $U_{\alpha_1, \beta_1, \alpha_2, \beta_2}$ might flip the contents of the registers L_1 and L_2 depending on the values of $\alpha_1, \beta_1, \alpha_2$ and β_2 . This enables L to keep track of the noise introduced to a pair.

There are two approaches how L can apply the noise maps $U_{\alpha_1, \beta_1, \alpha_2, \beta_2}$: stochastically in terms of CPTP maps, or coherently in terms of unitaries acting on an enlarged Hilbert space. Here we assume the latter approach, but provide the analysis of the noisy DEJMPS protocol in terms of CPTP maps and purifications.

To show that these are equivalent, first suppose that L owns a register H set to the state $\sum_{\alpha_1, \beta_1, \alpha_2, \beta_2} \sqrt{\tilde{f}_{\alpha_1, \beta_1, \alpha_2, \beta_2}} |\alpha_1 \beta_1 \alpha_2 \beta_2\rangle_H$ where $\tilde{f}_{\alpha_1, \beta_1, \alpha_2, \beta_2}$ are the probabilities of applying the respective noise map $U_{\alpha_1, \beta_1, \alpha_2, \beta_2}$. L uses the register H to apply the noise maps $U_{\alpha_1, \beta_1, \alpha_2, \beta_2}$ coherently controlled to the input state

$|\Psi\rangle_{ABEL}$. We observe that tracing out H after applying all the noise maps $U_{\alpha_1, \beta_1, \alpha_2, \beta_2}$ in a controlled fashion yields

$$\sum_{\alpha_1, \beta_1, \alpha_2, \beta_2} \tilde{f}_{\alpha_1, \beta_1, \alpha_2, \beta_2} U_{\alpha_1, \beta_1, \alpha_2, \beta_2} (|\Psi\rangle \langle \Psi| \otimes |\Psi\rangle \langle \Psi|) U_{\alpha_1, \beta_1, \alpha_2, \beta_2}^\dagger.$$

On the other hand, assume that L applies the noise process in terms of a CPTP map N , i.e.

$$N\rho = \sum_{\alpha_1, \beta_1, \alpha_2, \beta_2} \tilde{f}_{\alpha_1, \beta_1, \alpha_2, \beta_2} U_{\alpha_1, \beta_1, \alpha_2, \beta_2} (|\Psi\rangle \langle \Psi| \otimes |\Psi\rangle \langle \Psi|) U_{\alpha_1, \beta_1, \alpha_2, \beta_2}^\dagger.$$

We observe that $N\rho$ will be, in general, a mixed state, thus there exists a purification on a larger Hilbert space. As all purifications are unitarily equivalent, see e.g. [29], we choose the purification

$$|\Phi\rangle = \sum_{\alpha_1, \beta_1, \alpha_2, \beta_2} \sqrt{\tilde{f}_{\alpha_1, \beta_1, \alpha_2, \beta_2}} U_{\alpha_1, \beta_1, \alpha_2, \beta_2} |\Psi\rangle \otimes |\Psi\rangle \otimes |\alpha_1 \beta_1 \alpha_2 \beta_2\rangle_H.$$

Hence $\text{tr}_H [|\Phi\rangle \langle \Phi|] = N\rho$. Furthermore, we observe that the pure state $|\Phi\rangle$ can be generated by applying the unitaries $U_{\alpha_1, \beta_1, \alpha_2, \beta_2}$, coherently controlled by the register H , to $|\Psi\rangle \otimes |\Psi\rangle \otimes \left(\sum_{\alpha_1, \beta_1, \alpha_2, \beta_2} \sqrt{\tilde{f}_{\alpha_1, \beta_1, \alpha_2, \beta_2}} |\alpha_1 \beta_1 \alpha_2 \beta_2\rangle_H \right)$.

This equivalence allows us to assume that L introduces the noise as a CPTP map, applying $U_{\alpha_1, \beta_1, \alpha_2, \beta_2}$ with respective probabilities $\tilde{f}_{\alpha_1, \beta_1, \alpha_2, \beta_2}$ and purifying the state after the basic step is executed by Alice and Bob.

Since the noise of L is applied before the basic distillation step is executed by Alice and Bob, the result of one noisy distillation step reads as

$$\rho' = \sum_{\alpha_1, \beta_1, \alpha_2, \beta_2} \tilde{f}_{\alpha_1, \beta_1, \alpha_2, \beta_2} U_u O'_{2\text{-EPP}} (U_{\alpha_1, \beta_1}^{(a_1)} \otimes U_{\alpha_2, \beta_2}^{(a_2)}) (|\Psi\rangle \langle \Psi| \otimes |\Psi\rangle \langle \Psi|) (U_{\alpha_1, \beta_1}^{(a_1)} \otimes U_{\alpha_2, \beta_2}^{(a_2)})^\dagger O_{2\text{-EPP}}'^\dagger U_u^\dagger. \quad (12)$$

which needs finally to be purified.

In order to evaluate (12), we proceed as follows:

- Step 1: We first compute

$$O'_{2\text{-EPP}} (U_{\alpha_1, \beta_1}^{(a_1)} \otimes U_{\alpha_2, \beta_2}^{(a_2)}) |\Psi\rangle \otimes |\Psi\rangle.$$

which corresponds to the state after the noise map $U_{\alpha_1, \beta_1}^{(a_1)} \otimes U_{\alpha_2, \beta_2}^{(a_2)}$ is applied by L and the basic step of the distillation protocol is executed by Alice and Bob.

- Step 2: We apply the unitary U_u , which acts only on L 's systems and whose purpose we clarify later, to the previous equality.
- Step 3: We have to determine the purification held by Eve if the noise is leaked to her. In doing so, we trace out Eve and then provide her with the purification of the resulting state (which corresponds to leaking the noise transcripts to Eve).

Step 1: We observe that applying the noise map $U_{\alpha, \beta}^{(a_1)}$ to $|\Psi\rangle$ yields

$$\begin{aligned} U_{\alpha, \beta}^{(a_1)} |\Psi\rangle &= U_{\alpha, \beta}^{(a_1)} \sum_{i, j, k, l} P_{ijkl} |B_{ij}\rangle_{AB} |kl\rangle_L |ijkl\rangle_E \\ &= \sum_{i, j, k, l} P_{ijkl} |B_{(i \oplus \alpha)(j \oplus \beta)}\rangle_{AB} |(k \oplus \alpha)(l \oplus \beta)\rangle_L |ijkl\rangle_E \\ &= \sum_{i, j, k, l} P_{(i \oplus \alpha)(j \oplus \beta)(k \oplus \alpha)(l \oplus \beta)} |B_{ij}\rangle_{AB} |kl\rangle_L |(i \oplus \alpha)(j \oplus \beta)(k \oplus \alpha)(l \oplus \beta)\rangle_E. \end{aligned} \quad (13)$$

This observation suggests the following notational simplifications:

$$P_{ijkl}^{\alpha\beta} = P_{(i \oplus \alpha)(j \oplus \beta)(k \oplus \alpha)(l \oplus \beta)} \quad \text{and} \quad |e_{ijkl}^{\alpha\beta}\rangle_E = |(i \oplus \alpha)(j \oplus \beta)(k \oplus \alpha)(l \oplus \beta)\rangle_E.$$

Using this notation we rewrite (13) as $U_{\alpha,\beta}^{(a_1)} |\Psi\rangle = \sum_{i,j,k,l} P_{ijkl}^{\alpha\beta} |B_{ij}\rangle_{AB} |kl\rangle_L \left| e_{ijkl}^{\alpha\beta} \right\rangle_E$. This is the state of Alice, Bob, L, and Eve after the noise map $U_{\alpha,\beta}^{(a_1)}$ is applied by L to the first pair. In order to compute (12) we define

$$\begin{aligned} |\Psi''_{\alpha_1,\beta_1,\alpha_2,\beta_2}\rangle &= (U_{\alpha_1,\beta_1}^{(a_1)} \otimes U_{\alpha_2,\beta_2}^{(a_2)}) |\Psi\rangle |\Psi\rangle \\ &= \sum_{i_1,j_1,i_2,j_2} \sum_{k_1,l_1,k_2,l_2} A_{i_1j_1k_1l_1}^{\alpha_1\beta_1} P_{i_2j_2k_2l_2}^{\alpha_2\beta_2} |B_{i_1j_1}\rangle_{AB_1} |B_{i_2j_2}\rangle_{AB_2} |k_1l_1\rangle_{L_1} |k_2l_2\rangle_{L_2} \\ &\quad \otimes \left| e_{i_1j_1k_1l_1}^{\alpha_1\beta_1} \right\rangle_{E_1} \left| e_{i_2j_2k_2l_2}^{\alpha_2\beta_2} \right\rangle_{E_2} \end{aligned}$$

which corresponds to the state after the noise map $U_{\alpha_1,\beta_1}^{(a_1)} \otimes U_{\alpha_2,\beta_2}^{(a_2)}$ is applied and

$$|\Psi'_{\alpha_1,\beta_1,\alpha_2,\beta_2}\rangle = U_u O_{2\text{-EPP}} |\Psi''_{\alpha_1,\beta_1,\alpha_2,\beta_2}\rangle \quad (14)$$

which is the state after the noise map $U_{\alpha_1,\beta_1}^{(a_1)} \otimes U_{\alpha_2,\beta_2}^{(a_2)}$, one basic distillation step and the update of L's noise register by U_u . Thus we rewrite (12) as

$$\rho' = \sum_{\alpha_1,\beta_1,\alpha_2,\beta_2} \tilde{f}_{\alpha_1,\beta_1,\alpha_2,\beta_2} |\Psi'_{\alpha_1,\beta_1,\alpha_2,\beta_2}\rangle \langle \Psi'_{\alpha_1,\beta_1,\alpha_2,\beta_2}|. \quad (15)$$

According to (14) Alice and Bob apply one basic step of the DEJMPS protocol to the state $|\Psi''_{\alpha_1,\beta_1,\alpha_2,\beta_2}\rangle$. Recall that step 1 of Protocol 1 maps $|B_{ij}\rangle$ to $|B_{i(i\oplus j)}\rangle$ and that step 2 maps $|B_{ij}\rangle |B_{i'j'}\rangle$ to $|B_{(i\oplus i')j}\rangle |B_{i'(j\oplus j')}\rangle$. Thus we conclude that after step 1 and 2 of Protocol 1 the state of Alice, Bob, L, and Eve is

$$\begin{aligned} \sum_{i_1,j_1,i_2,j_2} \sum_{k_1,l_1,k_2,l_2} P_{i_1j_1k_1l_1}^{\alpha_1\beta_1} P_{i_2j_2k_2l_2}^{\alpha_2\beta_2} |B_{(i_1\oplus i_2)(i_1\oplus j_1)}\rangle_{AB_1} |B_{i_2(i_1\oplus j_1\oplus i_2\oplus j_2)}\rangle_{AB_2} |k_1l_1\rangle_{L_1} |k_2l_2\rangle_{L_2} \\ \left| e_{i_1j_1k_1l_1}^{\alpha_1\beta_1} \right\rangle_{E_1} \left| e_{i_2j_2k_2l_2}^{\alpha_2\beta_2} \right\rangle_{E_2} \end{aligned} \quad (16)$$

Following Protocol 1, a σ_z -measurement of the target pair of the BCNOT, i.e. the subsystem AB_2 , is applied to (16). Next Alice and Bob communicate their respective measurement outcomes over a classic authentic channel. If the measurement outcomes coincide, Alice and Bob keep the source pair, i.e. subsystem AB_1 of step 2, else they discard both subsystems AB_1 and AB_2 . We assume that both measurements yield the outcome 1. If both measurement outcomes yield 0, no phase factor $(-1)^{i_2}$ would be required in the expression (17). The coinciding measurement outcomes imply $i_1 \oplus j_1 \oplus i_2 \oplus j_2 = 0$. To summarize, the state post-selected on the measurement outcomes 1 of Alice and Bob is

$$\sum_{i_1,j_1,i_2,j_2} \sum_{k_1,l_1,k_2,l_2} (-1)^{i_2} P_{i_1j_1k_1l_1}^{\alpha_1\beta_1} P_{i_2(i_1\oplus j_1\oplus i_2)k_2l_2}^{\alpha_2\beta_2} |B_{(i_1\oplus i_2)(i_1\oplus j_1)}\rangle_{AB_1} |k_1l_1\rangle_{L_1} |k_2l_2\rangle_{L_2} \left| e_{i_1j_1k_1l_1}^{\alpha_1\beta_1} \right\rangle_{E_1} \left| e_{i_2(i_1\oplus j_1\oplus i_2)k_2l_2}^{\alpha_2\beta_2} \right\rangle_{E_2}. \quad (17)$$

Step 2: Recall that L stores in its register attached to the pair of Alice and Bob the effective noise introduced. For that purpose we introduce the unitary U_u as well as an ancilla system L_3 set to the state $|00\rangle_{L_3}$. Applying U_u to all three registers of L yields $U_u |00\rangle |i\rangle |j\rangle |i'\rangle |j'\rangle = |u(i,j,i',j')\rangle |i\rangle |j\rangle |i'\rangle |j'\rangle$ where u is the so called flag update function defined in [17]. The function u returns the effective noise introduced on the source pair of step 2 of Protocol 1. Applying U_u to (17) gives

$$\begin{aligned} |\Psi'_{\alpha_1,\beta_1,\alpha_2,\beta_2}\rangle &= \sum_{i_1,j_1,i_2,j_2} \sum_{k_1,l_1,k_2,l_2} (-1)^{i_2} P_{i_1j_1k_1l_1}^{\alpha_1\beta_1} P_{i_2(i_1\oplus j_1\oplus i_2)k_2l_2}^{\alpha_2\beta_2} |B_{(i_1\oplus i_2)(i_1\oplus j_1)}\rangle_{AB_1} |k_1l_1\rangle_{L_1} |k_2l_2\rangle_{L_2} |u(k_1,l_1,k_2,l_2)\rangle_{L_3} \\ &\quad \left| e_{i_1j_1k_1l_1}^{\alpha_1\beta_1} \right\rangle_{E_1} \left| e_{i_2(i_1\oplus j_1\oplus i_2)k_2l_2}^{\alpha_2\beta_2} \right\rangle_{E_2}. \end{aligned}$$

We remind the reader that $|\Psi'_{\alpha_1,\beta_1,\alpha_2,\beta_2}\rangle$ is the state after the application of i) the noise map $U_{\alpha_1,\beta_1}^{(a_1)} \otimes U_{\alpha_2,\beta_2}^{(a_2)}$, ii) a basic distillation step, and iii) the update of L's noise register by U_u .

Step 3: Since the noise transcripts - by assumption for this analysis - leak to Eve, we attribute the systems L_1 and L_2 to Eve. In order to treat the most general situation, we assume that Eve holds a purification of $\text{tr}_{L_1,L_2,E_1,E_2} [\rho']$.

We determine this purification by computing $\rho'_1 = \text{tr}_{L_1, L_2} [\rho']$ and $\rho'_2 = \text{tr}_{E_1, E_2} [\rho'_1]$ and attribute the purification of ρ'_2 to Eve.

By the linearity of the partial trace we have

$$\rho'_1 = \text{tr}_{L_1, L_2} [\rho'] = \sum_{\alpha_1, \beta_1, \alpha_2, \beta_2} \tilde{f}_{\alpha_1, \beta_1, \alpha_2, \beta_2} \text{tr}_{L_1, L_2} \left[|\Psi'_{\alpha_1, \beta_1, \alpha_2, \beta_2}\rangle \langle \Psi'_{\alpha_1, \beta_1, \alpha_2, \beta_2}| \right].$$

It is useful to define $\rho'_{\alpha_1, \beta_1, \alpha_2, \beta_2} = \text{tr}_{L_1, L_2} \left[|\Psi'_{\alpha_1, \beta_1, \alpha_2, \beta_2}\rangle \langle \Psi'_{\alpha_1, \beta_1, \alpha_2, \beta_2}| \right]$ which evaluates to

$$\begin{aligned} \rho'_{\alpha_1, \beta_1, \alpha_2, \beta_2} &= \text{tr}_{L_1, L_2} \left[|\Psi'_{\alpha_1, \beta_1, \alpha_2, \beta_2}\rangle \langle \Psi'_{\alpha_1, \beta_1, \alpha_2, \beta_2}| \right] \\ &= \sum (-1)^{i_2 \oplus i'_2} P_{i_1 j_1 k_1 l_1}^{\alpha_1 \beta_1} P_{i_2 (i_1 \oplus j_1 \oplus i_2) k_2 l_2}^{\alpha_2 \beta_2} (P_{i'_1 j'_1 k'_1 l'_1}^{\alpha_1 \beta_1} P_{i'_2 (i'_1 \oplus j'_1 \oplus i'_2) k'_2 l'_2}^{\alpha_2 \beta_2})^* |B_{(i_1 \oplus i_2)(i_1 \oplus j_1)}\rangle \langle B_{(i'_1 \oplus i'_2)(i'_1 \oplus j'_1)}| \\ &\quad \otimes |u(k_1, l_1, k_2, l_2)\rangle \langle u(k_1, l_1, k_2, l_2)| \otimes |e_{i_1 j_1 k_1 l_1}^{\alpha_1 \beta_1}\rangle \langle e_{i'_1 j'_1 k'_1 l'_1}^{\alpha_1 \beta_1}| \otimes |e_{i_2 (i_1 \oplus j_1 \oplus i_2) k_2 l_2}^{\alpha_2 \beta_2}\rangle \langle e_{i'_2 (i'_1 \oplus j'_1 \oplus i'_2) k'_2 l'_2}^{\alpha_2 \beta_2}|. \end{aligned}$$

In the previous expression we neglected the indices appearing in the sum for simplicity, but it is understood that the sum ranges over all indices except $\alpha_1, \beta_1, \alpha_2$ and β_2 .

In order to determine the state of Alice, Bob, and L which Eve finally purifies we have to compute $\rho'_2 = \text{tr}_{E_1, E_2} [\rho'_1]$. Again, the linearity of the partial trace yields

$$\rho'_2 = \text{tr}_{E_1, E_2} [\rho'_1] = \sum_{\alpha_1, \beta_1, \alpha_2, \beta_2} \tilde{f}_{\alpha_1, \beta_1, \alpha_2, \beta_2} \text{tr}_{E_1, E_2} [\rho'_{\alpha_1, \beta_1, \alpha_2, \beta_2}]. \quad (18)$$

We remind the reader that $|e_{ijkl}^{\alpha\beta}\rangle_{E_1} = |(i \oplus \alpha)(j \oplus \beta)(k \oplus \alpha)(l \oplus \beta)\rangle_{E_1}$. Hence, for fixed α_1 and β_1 , we have $\text{tr} |e_{i_1 j_1 k_1 l_1}^{\alpha_1 \beta_1}\rangle \langle e_{i'_1 j'_1 k'_1 l'_1}^{\alpha_1 \beta_1}| = \delta_{i_1 i'_1} \delta_{j_1 j'_1}$, which implies that $i'_1 = i_1$ and $j'_1 = j_1$. Thus, we also have

$$\text{tr} |e_{i_2 (i_1 \oplus j_1 \oplus i_2) k_2 l_2}^{\alpha_2 \beta_2}\rangle \langle e_{i'_2 (i'_1 \oplus j'_1 \oplus i'_2) k'_2 l'_2}^{\alpha_2 \beta_2}| = \text{tr} |e_{i_2 (i_1 \oplus j_1 \oplus i_2) k_2 l_2}^{\alpha_2 \beta_2}\rangle \langle e_{i'_2 (i_1 \oplus j_1 \oplus i_2) k_2 l_2}^{\alpha_2 \beta_2}| = \delta_{i_2 i'_2}.$$

Hence

$$\begin{aligned} \text{tr}_{E_1, E_2} [\rho'_{\alpha_1, \beta_1, \alpha_2, \beta_2}] &= \\ &= \sum_{i_1, i_2, j_1} \sum_{k_1, l_1, k_2, l_2} P_{i_1 j_1 k_1 l_1}^{\alpha_1 \beta_1} P_{i_2 (i_1 \oplus j_1 \oplus i_2) k_2 l_2}^{\alpha_2 \beta_2} (P_{i_1 j_1 k_1 l_1}^{\alpha_1 \beta_1} P_{i_2 (i_1 \oplus j_1 \oplus i_2) k_2 l_2}^{\alpha_2 \beta_2})^* \\ &\quad |B_{(i_1 \oplus i_2)(i_1 \oplus j_1)}\rangle \langle B_{(i_1 \oplus i_2)(i_1 \oplus j_1)}| \otimes |u(k_1, l_1, k_2, l_2)\rangle \langle u(k_1, l_1, k_2, l_2)| \\ &= \sum_{i_1, i_2, j_1} \sum_{k_1, l_1, k_2, l_2} \left| P_{i_1 j_1 k_1 l_1}^{\alpha_1 \beta_1} P_{i_2 (i_1 \oplus j_1 \oplus i_2) k_2 l_2}^{\alpha_2 \beta_2} \right|^2 \\ &\quad |B_{(i_1 \oplus i_2)(i_1 \oplus j_1)}\rangle \langle B_{(i_1 \oplus i_2)(i_1 \oplus j_1)}| \otimes |u(k_1, l_1, k_2, l_2)\rangle \langle u(k_1, l_1, k_2, l_2)|. \end{aligned} \quad (19)$$

By inserting (19) in (18) we get

$$\begin{aligned}
\rho'_2 &= \text{tr}_{E_1, E_2} [\rho'_1] \\
&= \sum_{\alpha_1, \beta_1, \alpha_2, \beta_2} \tilde{f}_{\alpha_1, \beta_1, \alpha_2, \beta_2} \text{tr}_{E_1, E_2} [\rho'_{\alpha_1, \beta_1, \alpha_2, \beta_2}] \\
&= \sum_{\alpha_1, \beta_1, \alpha_2, \beta_2} \tilde{f}_{\alpha_1, \beta_1, \alpha_2, \beta_2} \sum_{i_1, i_2, j_1} \sum_{k_1, l_1, k_2, l_2} \left| P_{i_1 j_1 k_1 l_1}^{\alpha_1 \beta_1} P_{i_2 (i_1 \oplus j_1 \oplus i_2) k_2 l_2}^{\alpha_2 \beta_2} \right|^2 \\
&\quad \left| B_{(i_1 \oplus i_2)(i_1 \oplus j_1)} \right\rangle \left\langle B_{(i_1 \oplus i_2)(i_1 \oplus j_1)} \right| \otimes |u(k_1, l_1, k_2, l_2)\rangle \langle u(k_1, l_1, k_2, l_2)| \\
&= \sum_{i_1, i_2, j_1} \left| B_{(i_1 \oplus i_2)(i_1 \oplus j_1)} \right\rangle \left\langle B_{(i_1 \oplus i_2)(i_1 \oplus j_1)} \right| \otimes \sum_{\gamma_0, \gamma_1} \left(\sum_{\substack{\alpha_1, \beta_1, \alpha_2, \beta_2, k_1, l_1, k_2, l_2 \\ u(k_1, l_1, k_2, l_2) = (\gamma_0, \gamma_1)}} \tilde{f}_{\alpha_1, \beta_1, \alpha_2, \beta_2} \left| P_{i_1 j_1 k_1 l_1}^{\alpha_1 \beta_1} P_{i_2 (i_1 \oplus j_1 \oplus i_2) k_2 l_2}^{\alpha_2 \beta_2} \right|^2 \right) \\
&\quad |\gamma_0 \gamma_1\rangle \langle \gamma_0 \gamma_1|.
\end{aligned}$$

Rearranging the sum over i_1, i_2 and j_1 in the previous equation gives

$$\sum_{\delta_0, \delta_1} |B_{\delta_0 \delta_1}\rangle \langle B_{\delta_0 \delta_1}| \otimes \sum_{\gamma_0, \gamma_1} \left(\sum_{\substack{i_1, i_2, j_1 \\ i_1 \oplus i_2 = \delta_0, i_1 \oplus j_1 = \delta_1}} \sum_{\substack{\alpha_1, \beta_1, \alpha_2, \beta_2, k_1, l_1, k_2, l_2 \\ u(k_1, l_1, k_2, l_2) = (\gamma_0, \gamma_1)}} \tilde{f}_{\alpha_1, \beta_1, \alpha_2, \beta_2} \left| P_{i_1 j_1 k_1 l_1}^{\alpha_1 \beta_1} P_{i_2 (i_1 \oplus j_1 \oplus i_2) k_2 l_2}^{\alpha_2 \beta_2} \right|^2 \right) |\gamma_0 \gamma_1\rangle \langle \gamma_0 \gamma_1|. \quad (20)$$

Using the definition

$$|\tilde{P}_{\delta_0 \delta_1 \gamma_0 \gamma_1}|^2 = \sum_{\substack{i_1, i_2, j_1 \\ i_1 \oplus i_2 = \delta_0, i_1 \oplus j_1 = \delta_1}} \sum_{\substack{\alpha_1, \beta_1, \alpha_2, \beta_2, k_1, l_1, k_2, l_2 \\ u(k_1, l_1, k_2, l_2) = (\gamma_0, \gamma_1)}} \tilde{f}_{\alpha_1, \beta_1, \alpha_2, \beta_2} \left| P_{i_1 j_1 k_1 l_1}^{\alpha_1 \beta_1} P_{i_2 (i_1 \oplus j_1 \oplus i_2) k_2 l_2}^{\alpha_2 \beta_2} \right|^2 \quad (21)$$

where $\delta_0, \delta_1, \gamma_0, \gamma_1 \in \{0, 1\}$ and omitting the normalization factor for clarity, (20) simplifies to

$$\sum_{\delta_0, \delta_1} |B_{\delta_0 \delta_1}\rangle \langle B_{\delta_0 \delta_1}| \otimes \sum_{\gamma_0, \gamma_1} |\tilde{P}_{\delta_0 \delta_1 \gamma_0 \gamma_1}|^2 |\gamma_0 \gamma_1\rangle \langle \gamma_0 \gamma_1|$$

which is the state of Alice, Bob, and L after one noisy distillation step. Since this final state is purified by Eve with the leaked noise transcripts and all purifications are unitarily equivalent, the state of Alice, Bob, L, and Eve after one noisy distillation step can be written without loss of generality as

$$|\psi^{DEJMPS}\rangle = \sum_{\delta_0, \delta_1, \gamma_0, \gamma_1} \tilde{P}_{\delta_0, \delta_1, \gamma_0, \gamma_1} |B_{\delta_0, \delta_1}\rangle_{AB} |\gamma_0 \gamma_1\rangle_L |\delta_0 \delta_1 \gamma_0 \gamma_1\rangle_E.$$

This also implies that (21) are the recurrence relations of the noisy DEJMPS protocol.

Fixed point and convergence - Binary pairs

First we study the scaling of the systems of Alice, Bob, and L and extend those results then to the (possibly leaked) noise transcripts of Eve in terms of purifications.

Suppose that the initial i.i.d. pairs of Alice and Bob are mixtures of $|B_{00}\rangle$ and $|B_{01}\rangle$ and that L applies either the identity or a σ_x -operator with respective probabilities \tilde{f}_0 and $\tilde{f}_1 = 1 - \tilde{f}_0$ independently to each pair. We remind the reader that Eve purifies the state of Alice, Bob, and L with the leaked noise transcripts, i.e. each individual state

taking Eve into account at an intermediate round of the DEJMPS protocol reads as $\sum_{i,j} P_{ij} |B_{0i}\rangle_{AB} \otimes |\eta_j\rangle_L \otimes |\eta_{ij}\rangle_E$. Using $p_{ij} = |P_{ij}|^2$, the recurrence relations (21) for the setting we are concerned with here simplify to

$$\tilde{p}_{00} = 1/N(\tilde{f}_0^2(p_{00}^2 + 2p_{00}p_{01}) + \tilde{f}_1^2(p_{11}^2 + 2p_{10}p_{11}) + 2\tilde{f}_0\tilde{f}_1(p_{11}p_{00} + p_{10}p_{00} + p_{11}p_{01})), \quad (22)$$

$$\tilde{p}_{01} = 1/N(\tilde{f}_0^2 p_{01}^2 + 2\tilde{f}_0\tilde{f}_1 p_{10}p_{01} + \tilde{f}_1^2 p_{10}^2), \quad (23)$$

$$\tilde{p}_{10} = 1/N(\tilde{f}_0^2(p_{10}^2 + 2p_{10}p_{11}) + \tilde{f}_1^2(p_{01}^2 + 2p_{00}p_{01}) + 2\tilde{f}_0\tilde{f}_1(p_{01}p_{10} + p_{00}p_{10} + p_{01}p_{11})), \quad (24)$$

$$\tilde{p}_{11} = 1/N(\tilde{f}_0^2 p_{11}^2 + 2\tilde{f}_0\tilde{f}_1 p_{00}p_{11} + \tilde{f}_1^2 p_{00}^2). \quad (25)$$

where $N = (\tilde{f}_0^2 + \tilde{f}_1^2)((p_{00} + p_{01})^2 + (p_{10} + p_{11})^2) + 4\tilde{f}_0\tilde{f}_1(p_{00} + p_{01})(p_{10} + p_{11})$. In the following we denote the recurrence relations (22)–(25) by the vector-valued mapping \mathbf{f} , i.e. $\mathbf{p} \xrightarrow{\mathbf{f}} \tilde{\mathbf{p}}$, where $\mathbf{p} = (p_{00}, p_{01}, p_{10}, p_{11})$. A simple computation yields the following fixed points of \mathbf{f} :

$$p_{00}^\infty = 1/2 + \sqrt{4\tilde{f}_0 - 3}/(4\tilde{f}_0 - 2) \quad p_{01}^\infty = p_{10}^\infty = 0 \quad p_{11}^\infty = 1 - p_{00}^\infty, \quad (26)$$

$$p_{00}^\infty = 1/2 - \sqrt{4\tilde{f}_0 - 3}/(4\tilde{f}_0 - 2) \quad p_{01}^\infty = p_{10}^\infty = 0 \quad p_{11}^\infty = 1 - p_{00}^\infty, \quad (27)$$

$$p_{00}^\infty = p_{11}^\infty = 1/2 \quad p_{01}^\infty = p_{10}^\infty = 0. \quad (28)$$

The parameter estimation phase guarantees that the fidelity F with $|B_{00}\rangle$ is sufficiently high for distillation. Hence the fixed point of interest is (26), i.e.

$$\mathbf{p}^\infty = (1/2 + \sqrt{4\tilde{f}_0 - 3}/(4\tilde{f}_0 - 2), 0, 0, 1/2 - \sqrt{4\tilde{f}_0 - 3}/(4\tilde{f}_0 - 2)). \quad (29)$$

From (29) we observe that in the limit the ‘cross-probabilities’ p_{01} and p_{10} , vanish, hence L is fully correlated to AB . It is of central importance, regarding convergence that the fixed point \mathbf{p}^∞ is an attractor, as only this ensures convergence towards that fixed point. Note that \mathbf{p}^∞ is an attractor if and only if the largest eigenvalue λ_{max} of $\mathbf{f}'(\mathbf{p}^\infty)$ satisfies $\lambda_{max} < 1$. We easily find that $\lambda_{max} = (\tilde{f}_0\sqrt{4\tilde{f}_0 - 3} - \tilde{f}_0)/(2\tilde{f}_0 - 1) < 1$ for $0.78 \leq \tilde{f}_0 \leq 1$.

The fixed point \mathbf{p}^∞ enables us to determine the rate of convergence. For that purpose, we expand \mathbf{f} in terms of its Taylor series around the fixed point \mathbf{p}^∞ , i.e. $\tilde{\mathbf{p}} = \mathbf{f}(\mathbf{p}) \approx \mathbf{f}(\mathbf{p}^\infty) + \mathbf{f}'(\mathbf{p}^\infty)(\mathbf{p} - \mathbf{p}^\infty)$. Hence by defining $\mathbf{e} = \mathbf{p} - \mathbf{p}^\infty$ we find $\tilde{\mathbf{e}} = \mathbf{f}'(\mathbf{p}^\infty)\mathbf{e}$, providing an estimate of the error propagation for one successful distillation round. The state of Alice, Bob, and L after n successful distillation rounds and at the fixpoint read as $\rho_n = \sum_{ij} p_{ij}^{(n)} |B_{0i}\rangle \langle B_{0i}|_{AB} \otimes |\eta_j\rangle \langle \eta_j|_L$ and $\rho_{\text{fix}} = \sum_i p_{ii}^\infty |B_{0i}\rangle \langle B_{0i}|_{AB} \otimes |\eta_i\rangle \langle \eta_i|_L$ respectively, which implies for their distance induced by the 1-norm

$$\varepsilon_n = \|\rho_n - \rho_{\text{fix}}\|_1 = \left\| \sum_{ij} (p_{ij}^{(n)} - p_{ij}^\infty) |B_{0i}\rangle \langle B_{0i}|_{AB} \otimes |\eta_j\rangle \langle \eta_j|_L \right\|_1 = \underbrace{\sum_{ij} |p_{ij}^{(n)} - p_{ij}^\infty|}_{\|\mathbf{e}_n\|_{1,v}} \leq \|\mathbf{f}'(\mathbf{p}^\infty)^{n-1}\| \|\mathbf{e}_1\|_{1,v}. \quad (30)$$

where $\|\mathbf{x}\|_{1,v} = \sum_{i=1}^k |x_i|$ denotes the 1-norm of vectors in \mathbb{C}^k .

Eq. (30) only concerns the systems of Alice, Bob, and L . To complete the analysis we recall that Eve purifies ρ_n and ρ_{fix} with the leaked noise transcripts of L . If we take this purifying system, E , into account, i.e. consider $\|\psi^n\rangle \langle \psi^n|_{ABEL} - |\psi^\alpha\rangle \langle \psi^\alpha|_{ABEL}\|_1$ where $\rho_n = \text{tr}_E[|\psi^n\rangle \langle \psi^n|_{ABEL}]$, $|\psi^\alpha\rangle_{ABEL} = \sum_{i,j} P_{ij}^\infty |B_{0i}\rangle_{AB} \otimes |\eta_j\rangle_L \otimes |\eta_{ij}\rangle_E$ with $|P_{ij}^\infty|^2 = p_{ij}^\infty$ and $\rho_{\text{fix}} = \text{tr}_E[|\psi^\alpha\rangle \langle \psi^\alpha|_{ABEL}]$, we find

$$\|\psi^n\rangle \langle \psi^n|_{ABEL} - |\psi^\alpha\rangle \langle \psi^\alpha|_{ABEL}\|_1 \leq \sqrt{\varepsilon_n} \quad (31)$$

since purifications scale with a square root.

In order to apply the post-selection-based reduction, we need to relate the previously obtained results for i.i.d. input pairs to general ensembles. We remind the reader, as we have stated in the main text, that for all purifications $|\psi\rangle_{ABE'}$ of a n -partite input state ρ_{AB} we have

$$\|(\mathcal{E} \otimes id_{E'}) (|\psi\rangle \langle \psi|_{ABE'}) - (\mathcal{F} \otimes id_{E'}) (|\psi\rangle \langle \psi|_{ABE'})\|_1 \leq 4g_{n,d} \sqrt{\max_{\sigma_{AB}} \|(\mathcal{E}_L - \mathcal{F}_L)(\sigma_{AB}^{\otimes n})\|_1} \quad (32)$$

where $g_{n,d} = \binom{n+d^2-1}{n}$. Thus, inserting the previous result for 2^n i.i.d. input states (necessary to achieve n rounds of distillation) in (32) yields

$$\|(\mathcal{E} \otimes id_{E'})(|\psi\rangle\langle\psi|_{ABE'}) - (\mathcal{F} \otimes id_{E'})(|\psi\rangle\langle\psi|_{ABE'})\|_1 \leq 4g_{2^n,d}\varepsilon_n^{1/4}.$$

One square root in the expression above arises from inequality (31) and the other square root appears from inequality (32).

Hence, for confidentiality we necessarily need $g_{2^n,d}\varepsilon_n^{1/4} \rightarrow 0$ for $n \rightarrow \infty$. Thus $\varepsilon_n^{1/4}$ should decay faster than $g_{2^n,d}$ grows in n . Numerical simulations suggest that, for $\tilde{f}_0 = 1 - 10^{-19}$, this turns out to be true, i.e. the post-selection-based reduction is applicable (see Figure 3). As stated in the main text such rates are unlikely to be achievable on the physical level, but they are, at least in principle, possible through fault-tolerant constructions.

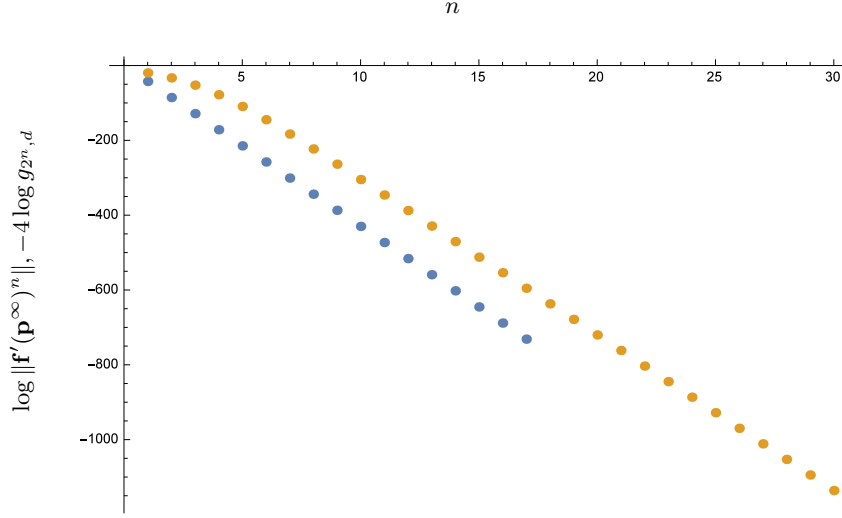


FIG. 3. The figure illustrates $\log \|\mathbf{f}'(\mathbf{p}^\infty)^n\|$ (blue) and $-4 \log g_{2^n,d}$ (yellow) for the binary pairs and $\tilde{f}_0 = 1 - 10^{-19}$.

Fixed point and convergence - General pairs

In the following we show that the previous established results also hold true for the general i.i.d. setting where L applies all four Pauli operators and each individual pair is arbitrary. We remind the reader that the recurrence relations for states $\sum_{i,j,k,l} P_{ijkl} |B_{ij}\rangle_{AB} \otimes |\eta_{kl}\rangle_L \otimes |\eta_{ijkl}\rangle_E$ (i.e. Eve purifies $\rho_n = \sum_{i,j,k,l} |P_{ijkl}|^2 |B_{ij}\rangle\langle B_{ij}|_{AB} \otimes |\eta_{kl}\rangle\langle\eta_{kl}|_L$ with the leaked noise transcripts) read (by denoting $|P_{ijkl}|^2 = p_{ijkl}$) as

$$\tilde{p}_{\delta_0\delta_1\gamma_0\gamma_1} = \sum_{\substack{i_1,i_2,j_1 \\ i_1 \oplus i_2 = \delta_0, i_1 \oplus j_1 = \delta_1}} \sum_{\substack{\alpha_1,\beta_1,\alpha_2,\beta_2,k_1,l_1,k_2,l_2 \\ u(k_1,l_1,k_2,l_2) = (\gamma_0,\gamma_1)}} \tilde{f}_{\alpha_1,\beta_1,\alpha_2,\beta_2} p_{(i_1 \oplus \alpha_1)(j_1 \oplus \beta_1)(k_1 \oplus \alpha_1)(l_1 \oplus \beta_1)} p_{(i_2 \oplus \alpha_2)(i_1 \oplus j_1 \oplus i_2 \oplus \beta_2)(k_2 \oplus \alpha_2)(l_2 \oplus \beta_2)}$$

modulo the normalization factor $\sum_{\delta_0\delta_1\gamma_0\gamma_1} \tilde{p}_{\delta_0\delta_1\gamma_0\gamma_1}$.

For simplicity we assume independent single qubit white noise, i.e. $\tilde{f}_{\alpha_1,\beta_1,\alpha_2,\beta_2} = \tilde{f}_{\alpha_1,\beta_1} \tilde{f}_{\alpha_2,\beta_2}$ as well as $\tilde{f}_{\alpha_1,\beta_1} = f$ if $\alpha_1 = \beta_1 = 0$ and $(1-f)/3$ otherwise. Furthermore, we assume that the initial fidelity F with $|B_{00}\rangle$ is sufficiently high for distillation. Numerically iterating the recurrence relations (which we again denote by $\mathbf{p} \xrightarrow{\mathbf{f}} \tilde{\mathbf{p}}$) reveal that, for a sufficiently large number of iterations, the ‘cross-probabilities’ vanish, i.e. $p_{ijkl}^\infty = 0 \Leftrightarrow i \neq k$ or $j \neq l$. Hence, to obtain a fixed point $\mathbf{p}^\infty = (p_{ijkl}^\infty)_{i,j,k,l=0}^1$ of \mathbf{f} , it is reasonable to assume that $p_{ijkl}^\infty = 0 \Leftrightarrow i \neq k$ or $j \neq l$.

Thus the fixed point \mathbf{p}^∞ is determined by four equations in four unknowns, namely the equations

$$p_{\delta_0 \delta_1 \delta_0 \delta_1} = \frac{1}{N} \sum_{\substack{i_1, i_2, j_1 \\ i_1 \oplus i_2 = \delta_0, i_1 \oplus j_1 = \delta_1}} \sum_{\substack{\alpha_1, \beta_1, \alpha_2, \beta_2 \\ u(i_1, j_1, i_2, i_1 \oplus j_1 \oplus i_2) = (\delta_1, \delta_1)}} \tilde{f}_{\alpha_1, \beta_1} \tilde{f}_{\alpha_2, \beta_2} P(i_1 \oplus \alpha_1)(j_1 \oplus \beta_1)(i_1 \oplus \alpha_1)(j_1 \oplus \beta_1) \\ \cdot P(i_2 \oplus \alpha_2)(i_1 \oplus j_1 \oplus i_2 \oplus \beta_2)(i_2 \oplus \alpha_2)(i_1 \oplus j_1 \oplus i_2 \oplus \beta_2).$$

where $\delta_0, \delta_1 \in \{0, 1\}$ and $N = \sum_{\delta_0, \delta_1} p_{\delta_0 \delta_1 \delta_0 \delta_1}$. Figure 4 illustrates the numerical estimate of p_{0000}^∞ as a function of f .

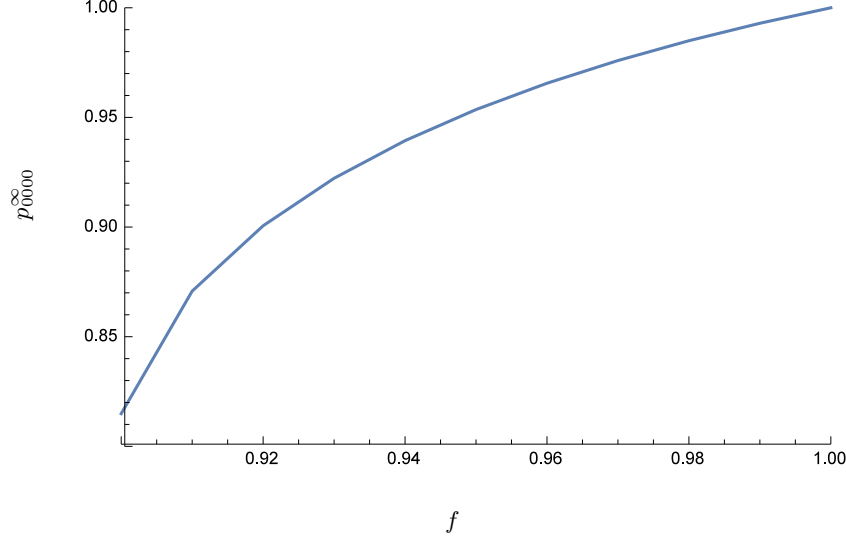


FIG. 4. The figure illustrates p_{0000}^∞ as a function of f . The fidelity with $|B_{00}\rangle$ of the asymptotic state is equal to unity for a perfect apparatus.

Similar to the case of binary pairs, we can write the recurrence relations \mathbf{f} in terms of its Taylor series expansion around the fixed point \mathbf{p}^∞ , i.e. $\tilde{\mathbf{p}} = \mathbf{f}(\mathbf{p}) \approx \mathbf{f}(\mathbf{p}^\infty) + \mathbf{f}'(\mathbf{p}^\infty)(\mathbf{p} - \mathbf{p}^\infty)$. Hence by defining $\mathbf{e} = \mathbf{p} - \mathbf{p}^\infty$ we have $\tilde{\mathbf{e}} = \mathbf{f}'(\mathbf{p}^\infty)\mathbf{e}$, i.e. as for binary pairs, the error induced by the 1-norm of the state of Alice, Bob, and L after n successful distillation rounds satisfies

$$\|\rho_n - \rho_{\text{fix}}\|_1 = \left\| \sum_{ijkl} \left(p_{ijkl}^{(n)} - p_{ijkl}^\infty \right) |B_{ij}\rangle \langle B_{ij}|_{AB} \otimes |\eta_{kl}\rangle \langle \eta_{kl}|_L \right\|_1 \leq \sum_{ijkl} \left| p_{ijkl}^{(n)} - p_{ijkl}^\infty \right| \leq \|\mathbf{f}'(\mathbf{p}^\infty)^{n-1}\| \|\mathbf{e}_1\|_{1;v}.$$

Figure 5 suggests a linear relationship between the number of successful distillation rounds n and $\log \|\mathbf{f}'(\mathbf{p}^\infty)^{n-1}\|$ for each noise level f , i.e. $b(f)n + a(f) = \log \|\mathbf{f}'(\mathbf{p}^\infty)^{n-1}\|$. As the number N of pairs necessary to achieve n distillation rounds is $N = 2^n$ ($\Leftrightarrow n = \log_2 N$) we have $b(f) \log_2 N + a(f) = \log \|\mathbf{f}'(\mathbf{p}^\infty)^{n-1}\|$, which is equivalent to

$$\|\mathbf{f}'(\mathbf{p}^\infty)^{n-1}\| = e^{a(f)} e^{b(f) \log_2 N} = a'(f) N^{b'(f)}.$$

Hence, $\|\mathbf{f}'(\mathbf{p}^\infty)^{n-1}\|$ scales as $F(N) \in O(N^{b'(f)})$ where $b'(f) < 0$ and $b'(f)$ decays for $f \rightarrow 1$.

What is left to show, is that the fixed point \mathbf{p}^∞ is an attracting fixed point. For that purpose we numerically compute the largest eigenvalue of $\mathbf{f}'(\mathbf{p}^\infty)$ and observe that, for noise below 10^{-1} , i.e. $1 - f < 10^{-1}$, the largest eigenvalue λ_{\max} of $\mathbf{f}'(\mathbf{p}^\infty)$ fulfills $\lambda_{\max} < 1$, proving that \mathbf{p}^∞ is an attracting fixed point.

This implies that, if the initial fidelity F with $|B_{00}\rangle$ is sufficiently large for distillation, the DEJMPS protocol necessarily converges towards the fixed point \mathbf{p}^∞ where the ‘cross-probabilities’ vanish.

The analysis so far still lacks Eve’s system E for the leaked noise transcripts. Suppose $|\psi^n\rangle_{ABEL}$ and $|\psi^f\rangle_{ABEL}$ are purifications of ρ_n and ρ_{fix} , i.e. $\rho_n = \text{tr}_E [|\psi^n\rangle \langle \psi^n|]$ and $\rho_{\text{fix}} = \text{tr}_E [|\psi^f\rangle \langle \psi^f|]$ respectively. This implies $\varepsilon_n = \||\psi^n\rangle \langle \psi^n| - |\psi^f\rangle \langle \psi^f|\|_1 \leq \sqrt{F(N)}$, i.e. $\varepsilon_n \in O(N^{b'(f)/2})$ which we also confirmed with our numeric results.

It is straightforward to extend the analysis above to two-qubit correlated white noise introduced by L on the system of Alice and Bob. Also in that case, similar results hold as we verified numerically.

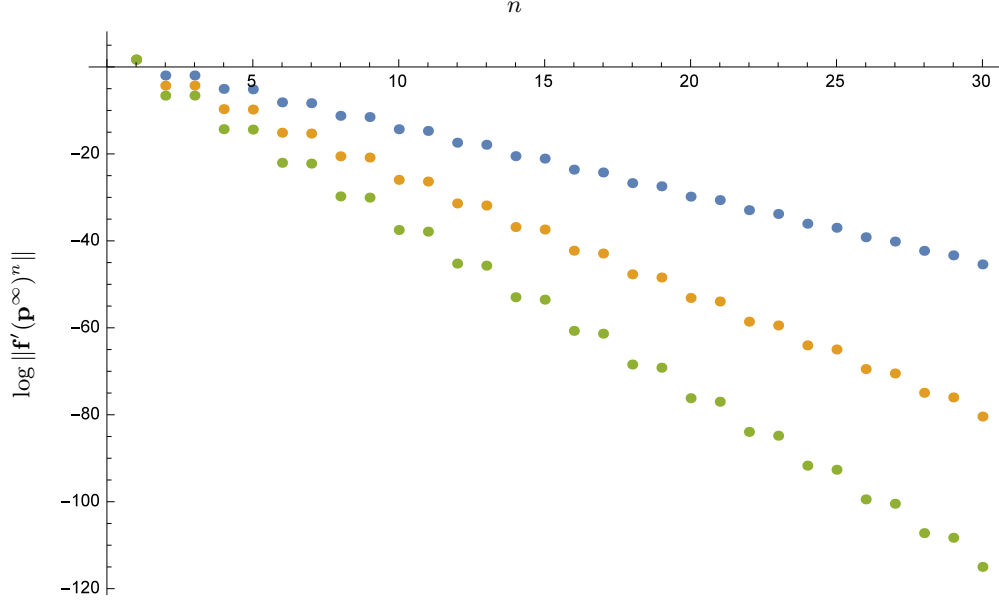


FIG. 5. The figure illustrates the value of $\log \|\mathbf{f}'(\mathbf{p}^\infty)^n\|$ as a function of successful distillation rounds for single qubit white noise 10^{-2} (blue), 10^{-3} (yellow) and 10^{-4} (green).

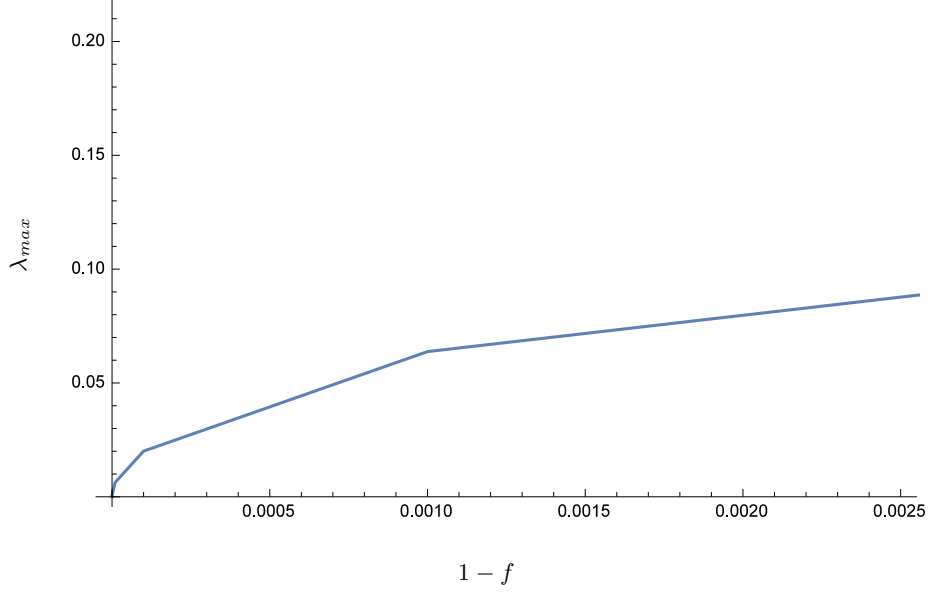


FIG. 6. The figure shows the largest eigenvalue of $\mathbf{f}'(\mathbf{p}^\infty)$ (y-axis) for single qubit white noise (x-axis)

The BBPSSW protocol

The protocol proposed in [28] (also referred to as BBPSSW protocol) is very similar to the DEJMPS protocol. Instead of step 1 of Protocol 1 Alice and Bob apply a correlated depolarization procedure (twirl) to their input states which brings them to Werner form.

For the subsequent analysis, suppose that each pair of Alice and Bob is of the form $\rho(p) = p|B_{00}\rangle\langle B_{00}| + (1-p)\frac{1}{4}id$. We assume that the apparatus applies independent and identical noise of the form $N\rho(p) = f\rho(p) + (1-f)/4(\rho(p) + \sigma_x\rho(p)\sigma_x + \sigma_y\rho(p)\sigma_y + \sigma_z\rho(p)\sigma_z)$ before each distillation step. In similar fashion to the DEJMPS protocol one easily

obtains the recurrence relation for the noisy BBPSSW protocol:

$$\tilde{p} = \frac{4p^2 f^2 + 2pf}{3p^2 f^2 + 3} = b(x).$$

The fixed point p^∞ of the protocol is obtained by solving the equation $b(p^\infty) = p^\infty$. A straightforward computation gives the fixed point $p^\infty = 2/3 + 1/3\sqrt{4 - 9/f^2 + 6/f}$ (which depends on the noise parameter f). It was shown in [27] that this fixed point is an attractor assuming sufficiently high initial fidelity with $|B_{00}\rangle$ per input pair. Expressing the recurrence relation b in terms of its Taylor series around p^∞ leads to

$$\tilde{p} = b(p) \approx b(p^\infty) + b'(p^\infty)(p - p^\infty). \quad (33)$$

Hence, (33) provides an approximation of the error in terms of fidelity with $|B_{00}\rangle$ after $n + 1$ successful distillation rounds, i.e. $\epsilon_{n+1} = (b'(p^\infty))^n \epsilon_1$. Moreover, we compute the first derivative of b by

$$b'(p) = \frac{2f(1 + 4fp - f^2 p^2)}{3(1 + f^2 p^2)^2}.$$

Evaluating b' at p^∞ yields

$$b'(p^\infty) = \frac{9 - 3f}{f(3 + 2(2 + \sqrt{4 - 9/f^2 + 6/f})f)}. \quad (34)$$

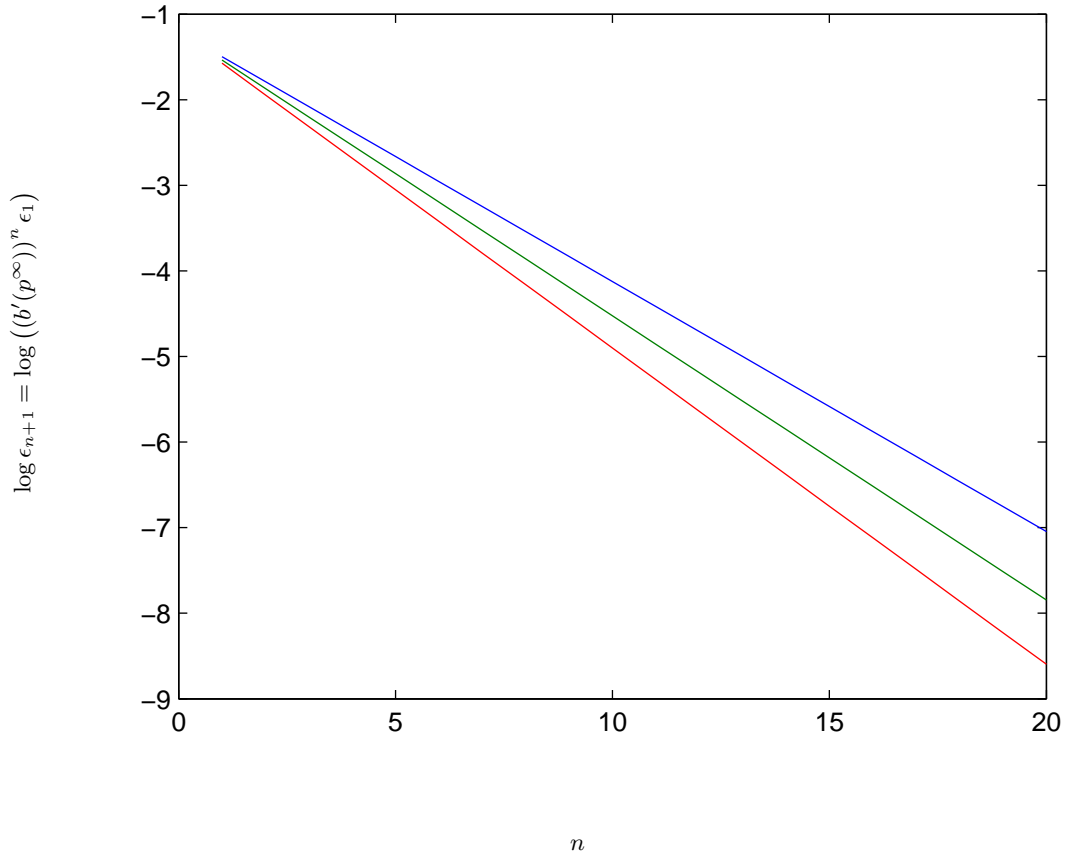


FIG. 7. The figure illustrates $\log \epsilon_{n+1}$ for the BBPSSW protocol for different noise parameters $f = 0.97$ (blue), $f = 0.98$ (green) and $f = 0.99$ (red).

From this we conclude that, if the apparatus is perfect, i.e. $f = 1$ in (34), the error in terms of fidelity with $|B_{00}\rangle$ after $n + 1$ successful distillation rounds scales as $\epsilon_{n+1} = (2/3)^n \epsilon_1$.

Using $\log_2 N = n$, where N denotes the number of input pairs, we infer for ϵ_{n+1} that

$$\epsilon_{n+1} = \epsilon_1 b'(p^\infty)^{\log_2 N} = \epsilon_1 \left(2^{\log_2 b'(p^\infty)} \right)^{\log_2 N} = \epsilon_1 N^{\log_2 b'(p^\infty)}.$$

This implies that ϵ_{n+1} scales as $F(N) \in O(N^{\log_2 b'(p^\infty)})$ and thus $\|\rho_{\text{fix}} - \rho_n\|_1$, where ρ_{fix} and ρ_n denote the fixed point and the state after n successful distillation rounds respectively, scales also as $F(N) \in O(N^{\log_2 b'(p^\infty)})$ as mentioned in the main text.

CONFIDENTIALITY OF ENTANGLEMENT DISTILLATION PROTOCOLS

In this section we give a proof of the factorization of Eve if the realized noise transcripts do not leak to her. The proof requires only one specific property of the real protocol \mathcal{E}^α : after passing the parameter estimation phase the distillation protocol always converges to *one* fixed point, i.e. the fixed point is *unique*, an *attractor* for all the states which pass the parameter estimation and depends on the noise parameters *only*.

Reduction for arbitrary noise levels via de-Finetti

We first state the following lemma which establishes a connection between measurements on one subsystem of a bipartite state and tensor product states.

Lemma 5. *[Steering of local states] Let ρ_{AB} be a bipartite (in general, mixed) state and let $\rho_A = \text{tr}_B[\rho_{AB}]$ and $\rho_B = \text{tr}_A[\rho_{AB}]$. Furthermore let ρ_B^ϕ be defined as*

$$\rho_B^\phi = \frac{\text{tr}_A[(|\phi\rangle\langle\phi| \otimes I)\rho_{AB}]}{p_A(\phi)}$$

where $|\phi\rangle \in \mathcal{H}_A$ and $p_A(\phi) = \text{tr}(|\phi\rangle\langle\phi| \rho_A)$. If $\|\rho_B^\phi - \rho_B\| \leq \epsilon$ for all $|\phi\rangle \in \mathcal{H}_A$, then

$$\|\rho_{AB} - \rho_A \otimes \rho_B\| \leq 2C\epsilon \quad (35)$$

where C only depends on the dimensions of A and B .

Proof. In the following we denote the four Pauli operators by

$$\sigma_0 = \text{id}, \quad \sigma_1 = \sigma_x, \quad \sigma_2 = \sigma_z, \quad \sigma_3 = \sigma_y.$$

First we decompose ρ_{AB} in the Pauli basis, i.e. we have

$$\rho_{AB} = \frac{1}{2^{a+b}} \sum_{\mathbf{i}, \mathbf{j}} \alpha_{\mathbf{ij}} \sigma_{\mathbf{i}} \otimes \sigma_{\mathbf{j}} \quad (36)$$

where a and b denote the dimension of A and B respectively and we use the notations $\mathbf{i} = (i_1, \dots, i_{4^n})$ and $\mathbf{j} = (j_1, \dots, j_{4^m})$ where each i_k and j_k are in $\{0, \dots, 3\}$ as well as $\sigma_{\mathbf{i}} = \bigotimes_{k=1}^{4^n} \sigma_{i_k}$ and $\sigma_{\mathbf{j}} = \bigotimes_{k=1}^{4^m} \sigma_{j_k}$. Recall that $\text{tr}(\sigma_0) = 2$ and $\text{tr}(\sigma_1) = \text{tr}(\sigma_2) = \text{tr}(\sigma_3) = 0$. From this one easily computes ρ_A and ρ_B by

$$\rho_A = \text{tr}_B[\rho_{AB}] = \frac{1}{2^{a+b}} \sum_{\mathbf{i}, \mathbf{j}} \alpha_{\mathbf{ij}} \sigma_{\mathbf{i}} \text{tr}(\sigma_{\mathbf{j}}) = \frac{1}{2^a} \sum_{\mathbf{i}} \alpha_{\mathbf{i}0} \sigma_{\mathbf{i}}, \quad (37)$$

$$\rho_B = \text{tr}_A[\rho_{AB}] = \frac{1}{2^{a+b}} \sum_{\mathbf{i}, \mathbf{j}} \alpha_{\mathbf{ij}} \text{tr}(\sigma_{\mathbf{i}}) \sigma_{\mathbf{j}} = \frac{1}{2^b} \sum_{\mathbf{j}} \alpha_{0\mathbf{j}} \sigma_{\mathbf{j}}. \quad (38)$$

Using (36), (37) and (38) we obtain for (35)

$$\begin{aligned} \|\rho_{AB} - \rho_A \otimes \rho_B\| &\leq \frac{1}{2^{a+b}} \sum_{\mathbf{i}, \mathbf{j}} \|(\alpha_{\mathbf{ij}} - \alpha_{\mathbf{i}0}\alpha_{0\mathbf{j}}) \sigma_{\mathbf{i}} \otimes \sigma_{\mathbf{j}}\| = \frac{1}{2^{a+b}} \sum_{\mathbf{i}, \mathbf{j}} |\alpha_{\mathbf{ij}} - \alpha_{\mathbf{i}0}\alpha_{0\mathbf{j}}| \cdot \|\sigma_{\mathbf{i}} \otimes \sigma_{\mathbf{j}}\| \\ &= \frac{2^{a+b}}{2^{a+b}} \sum_{\mathbf{i}, \mathbf{j}} |\alpha_{\mathbf{ij}} - \alpha_{\mathbf{i}0}\alpha_{0\mathbf{j}}| = \sum_{\mathbf{i}, \mathbf{j}} |\alpha_{\mathbf{ij}} - \alpha_{\mathbf{i}0}\alpha_{0\mathbf{j}}| = \|\mathbf{a} - \mathbf{a}'\|_{1; \mathbb{C}^{4^{n+m}}} \end{aligned} \quad (39)$$

where $\mathbf{a} = (\alpha_{00}, \dots, \alpha_{4^{n+m}})$, $\mathbf{a}' = (\alpha_{00}\alpha_{00}, \dots, \alpha_{4^{n+m}}\alpha_{4^{n+m}})$ and $\|\cdot\|_{1;\mathbb{C}^{4^{n+m}}}$ denotes the 1-norm of vectors in $\mathbb{C}^{4^{n+m}}$. Hence in order to prove (35) it is sufficient to prove $\|\mathbf{a} - \mathbf{a}'\|_{1;\mathbb{C}^{4^{n+m}}} \leq 2C\epsilon$. By assumption we have for ρ_B^ϕ where $|\phi\rangle \in \mathcal{H}_A$ and $p_A(\phi) = \text{tr}(|\phi\rangle\langle\phi| \otimes I \rho_{AB})$ that $\|\rho_B^\phi - \rho_B\| \leq \epsilon$ for all $|\phi\rangle \in \mathcal{H}_A$. Moreover, according to [29][Theorem 9.1] we have for all $|\xi\rangle \in \mathcal{H}_B$

$$\frac{1}{2}|p_B(\xi|\phi) - q_B(\xi)| = \frac{1}{2}|\text{tr}(|\xi\rangle\langle\xi| \rho_B^\phi) - \text{tr}(|\xi\rangle\langle\xi| \rho_B)| \leq \max_{E_m} \frac{1}{2} \sum_m |\text{tr}(E_m \rho_B^\phi) - \text{tr}(E_m \rho_B)| = \|\rho_B^\phi - \rho_B\| \leq \epsilon \quad (40)$$

where $p_B(\xi|\phi)$ denotes the conditional probability of obtaining the outcome ϕ on system A and the outcome ξ on system B and $\{E_m\}$ denotes a POVM on the subsystem of B . Suppose we perform a projective measurement on the systems of A and B denoted by $\{|\psi_k\rangle_{AB}\} = \{|\phi_k\rangle_A \otimes |\xi_k\rangle_B\}$ where $k \in \{1, \dots, 4^{n+m}\}$ on ρ_{AB} and $\rho_A \otimes \rho_B$. This yields for the respective probabilities $p_{AB}(\psi_k)$ and $q_{AB}(\psi_k)$ of observing outcome k for ρ_{AB} and $\rho_A \otimes \rho_B$

$$\begin{aligned} p_{AB}(\psi_k) &= \text{tr}(|\psi_k\rangle\langle\psi_k| \rho_{AB}) = \text{tr}(|\phi_k\rangle\langle\phi_k|_A \otimes |\xi_k\rangle\langle\xi_k|_B \rho_{AB}) = \text{tr}(|\xi_k\rangle\langle\xi_k|_B \text{tr}_A[(|\phi_k\rangle\langle\phi_k|_A \otimes I) \rho_{AB}]) \\ &= \text{tr}(|\xi_k\rangle\langle\xi_k|_B p_A(\phi_k) \rho_B^{\phi_k}) = p_A(\phi_k) \text{tr}(|\xi_k\rangle\langle\xi_k|_B \rho_B^{\phi_k}) = p_A(\phi_k) p_B(\xi_k|\phi_k), \\ q_{AB}(\psi_k) &= \text{tr}(|\psi_k\rangle\langle\psi_k| \rho_A \otimes \rho_B) = \text{tr}(|\phi_k\rangle\langle\phi_k|_A \otimes |\xi_k\rangle\langle\xi_k|_B \rho_A \otimes \rho_B) = q_A(\phi_k) q_B(\xi_k) \end{aligned}$$

where $p_B(\xi_k|\phi_k)$ denotes the conditional probability of obtaining outcome ϕ_k on system A first and obtaining outcome ξ_k on system B . We observe $p_A(\phi_k) = q_A(\phi_k)$. Thus we obtain

$$|p_{AB}(\psi_k) - q_{AB}(\psi_k)| = p_A(\phi_k) |p_B(\xi_k|\phi_k) - q_B(\xi_k)| \leq 2\epsilon p_A(\phi_k)$$

using (40). In order to compute a bound for (39) we use quantum state tomography, see e.g. [31]. For that purpose we perform an informationally complete POVM induced by different separable bases on $\mathcal{H}_A \otimes \mathcal{H}_B$. More precisely, we choose that many POVMs such that we have in total 4^{n+m} different outcomes. We observe for $|\psi_k\rangle_{AB} = |\phi_k\rangle_A \otimes |\xi_k\rangle_B$ that

$$p_{AB}(\psi_k) = \frac{1}{2^{a+b}} \sum_{\mathbf{i}, \mathbf{j}} \langle\phi_k|\sigma_{\mathbf{i}}|\phi_k\rangle \langle\xi_k|\sigma_{\mathbf{j}}|\xi_k\rangle \alpha_{\mathbf{i}\mathbf{j}} \quad \text{and} \quad q_{AB}(\psi_k) = \frac{1}{2^{a+b}} \sum_{\mathbf{i}, \mathbf{j}} \langle\phi_k|\sigma_{\mathbf{i}}|\phi_k\rangle \langle\xi_k|\sigma_{\mathbf{j}}|\xi_k\rangle \alpha_{\mathbf{i}0}\alpha_{0\mathbf{j}}. \quad (41)$$

Enumerating (41) for $1 \leq k \leq 4^{n+m}$ yields 4^{n+m} equations for \mathbf{a} , i.e.

$$p_{AB}(\psi_1) = \frac{1}{2^{a+b}} \sum_{\mathbf{i}, \mathbf{j}} \langle\phi_1|\sigma_{\mathbf{i}}|\phi_1\rangle \langle\xi_1|\sigma_{\mathbf{j}}|\xi_1\rangle \alpha_{\mathbf{i}\mathbf{j}}, \quad (42)$$

...

$$p_{AB}(\psi_{4^{n+m}}) = \frac{1}{2^{a+b}} \sum_{\mathbf{i}, \mathbf{j}} \langle\phi_{4^{n+m}}|\sigma_{\mathbf{i}}|\phi_{4^{n+m}}\rangle \langle\xi_{4^{n+m}}|\sigma_{\mathbf{j}}|\xi_{4^{n+m}}\rangle \alpha_{\mathbf{i}\mathbf{j}} \quad (43)$$

as well as 4^{n+m} equations for \mathbf{a}'

$$q_{AB}(\psi_1) = \frac{1}{2^{a+b}} \sum_{\mathbf{i}, \mathbf{j}} \langle\phi_1|\sigma_{\mathbf{i}}|\phi_1\rangle \langle\xi_1|\sigma_{\mathbf{j}}|\xi_1\rangle \alpha_{\mathbf{i}0}\alpha_{0\mathbf{j}}, \quad (44)$$

...,

$$q_{AB}(\psi_{4^{n+m}}) = \frac{1}{2^{a+b}} \sum_{\mathbf{i}, \mathbf{j}} \langle\phi_{4^{n+m}}|\sigma_{\mathbf{i}}|\phi_{4^{n+m}}\rangle \langle\xi_{4^{n+m}}|\sigma_{\mathbf{j}}|\xi_{4^{n+m}}\rangle \alpha_{\mathbf{i}0}\alpha_{0\mathbf{j}}. \quad (45)$$

We can rewrite the systems of equations (42)-(43) and (44)-(45) using

$$T = \begin{pmatrix} \langle\phi_1|\sigma_0|\phi_1\rangle \langle\xi_1|\sigma_0|\xi_1\rangle & \dots & \langle\phi_1|\sigma_{4^n}|\phi_1\rangle \langle\xi_1|\sigma_{4^m}|\xi_1\rangle \\ \dots & \dots & \dots \\ \langle\phi_{4^{n+m}}|\sigma_0|\phi_{4^{n+m}}\rangle \langle\xi_{4^{n+m}}|\sigma_0|\xi_{4^{n+m}}\rangle & \dots & \langle\phi_{4^{n+m}}|\sigma_{4^n}|\phi_{4^{n+m}}\rangle \langle\xi_{4^{n+m}}|\sigma_{4^m}|\xi_{4^{n+m}}\rangle \end{pmatrix}$$

and $\mathbf{p} = (p_{AB}(\psi_1), \dots, p_{AB}(\psi_{4^{n+m}}))$ and $\mathbf{q} = (q_{AB}(\psi_1), \dots, q_{AB}(\psi_{4^{n+m}}))$ as

$$\mathbf{p} = T\mathbf{a} \quad \text{and} \quad \mathbf{q} = T\mathbf{a}'$$

respectively. Hence $\mathbf{p} - \mathbf{q} = T(\mathbf{a} - \mathbf{a}')$. Moreover we observe that T is invertible if the POVM is informationally complete, see [31] for details. Thus, inverting T and taking norms on both sides yields

$$\|\mathbf{a} - \mathbf{a}'\|_{1;\mathbb{C}^{4^{n+m}}} \leq \|T^{-1}\| \|\mathbf{p} - \mathbf{q}\|_{1;\mathbb{C}^{4^{n+m}}} = \|T^{-1}\| \sum_k |p_{AB}(\psi_k) - q_{AB}(\psi_k)| \leq \|T^{-1}\| \sum_k 2\epsilon p_A(\phi_k) \leq 2\|T^{-1}\| 4^{n+m} \epsilon$$

which completes the proof with $C = \|T^{-1}\| 4^{n+m}$. \square

Roughly speaking Lemma 5 states that if all post-selected reduced states of a bipartite state are η -close then the overall state is $2\|T^{-1}\| 4^{n+m} \eta$ close to a product state.

In the following we use the definition of an ideal protocol if the noise maps do not leak to Eve, i.e. we define the ideal protocol \mathcal{F} for input $|\psi\rangle$ prepared by Eve through

$$(\mathcal{F} \otimes id_E)(|\psi\rangle\langle\psi|) = p_\rho \sigma_{AB}^\alpha \otimes \sigma_E \otimes |ok\rangle\langle ok| + (1 - p_\rho) \sigma_{AB}^\perp \otimes \sigma_E \otimes |fail\rangle\langle fail|$$

where σ_{AB}^α denotes the fixed point of the distillation protocol.

Before we are able to prove Lemma 2 of the main text we require the convergence of entanglement distillation protocols towards a unique and attracting fixed point depending on the noise parameter only for arbitrary inputs. Usually such an analysis is restricted to i.i.d. inputs, but we easily extend it to arbitrary inputs via the following Lemma.

Lemma 6. *Let $n, k \in \mathbb{N}$ where $k \leq n$. Furthermore, let $\mathcal{E}^{s\&t}$ be the real protocol and $\mathcal{F}^{s\&t}$ the ideal protocol as defined in the main text including symmetrization and the tracing out of $n - k$ pairs. Moreover, let ρ_{AB} be a n -partite mixed state shared by Alice and Bob and let \mathcal{F}' and \mathcal{E}' denote the real and ideal protocol after symmetrization and tracing out $n - k$ pairs. Then*

$$\|\mathcal{E}^{s\&t}(\rho_{AB}) - \mathcal{F}^{s\&t}(\rho_{AB})\|_1 \leq \frac{64k}{n} + \max_{\sigma_{AB}} \|\mathcal{E}'(\sigma_{AB}^{\otimes k}) - \mathcal{F}'(\sigma_{AB}^{\otimes k})\|_1 \quad (46)$$

Proof. Let ρ_{AB} be a mixed state. After Alice and Bob apply a symmetrization they share a permutation invariant state $\tilde{\rho}_{AB}$. Thus we can apply Theorem II.7 of [24] and have for $\xi_{AB}^k := \text{tr}_{n-k}[\tilde{\rho}_{AB}]$ the inequality $\|\xi_{AB}^k - \int \sigma_{AB}^{\otimes k} dm(\sigma_{AB})\|_1 \leq 32k/n$ for some probability measure m on the set of mixed states on AB . Moreover we note that \mathcal{E}' and \mathcal{F}' are CPTP maps. We define $\tau_k := \int \sigma_{AB}^{\otimes k} dm(\sigma_{AB})$. A straightforward computation shows

$$\begin{aligned} \|\mathcal{E}^{s\&t}(\rho_{AB}) - \mathcal{F}^{s\&t}(\rho_{AB})\|_1 &= \|\mathcal{E}'(\xi_{AB}^k) - \mathcal{F}'(\xi_{AB}^k)\|_1 \leq \|\mathcal{E}'(\xi_{AB}^k) - \mathcal{E}'(\tau_k)\|_1 + \|\mathcal{E}'(\tau_k) - \mathcal{F}'(\xi_{AB}^k)\|_1 \\ &\leq \|\mathcal{E}'(\xi_{AB}^k) - \mathcal{E}'(\tau_k)\|_1 + \|\mathcal{E}'(\tau_k) - \mathcal{F}'(\tau_k)\|_1 + \|\mathcal{F}'(\tau_k) - \mathcal{F}'(\xi_{AB}^k)\|_1 \\ &\leq 2\|\tau_k - \xi_{AB}^k\|_1 + \|\mathcal{E}'(\tau_k) - \mathcal{F}'(\tau_k)\|_1 \leq \frac{64k}{n} + \left\| (\mathcal{E}' - \mathcal{F}') \left(\int \sigma_{AB}^{\otimes k} dm(\sigma_{AB}) \right) \right\|_1 \\ &\leq \frac{64k}{n} + \max_{\sigma_{AB}} \|(\mathcal{E}' - \mathcal{F}')(\sigma_{AB}^{\otimes k})\|_1 \end{aligned}$$

which completes the proof. \square

We observe, that the right side of (46) is independent of the real and ideal protocols input. Thus we deduce

$$\max_{\rho_{AB}} \|\mathcal{E}^{s\&t}(\rho_{AB}) - \mathcal{F}^{s\&t}(\rho_{AB})\|_1 \leq \frac{64k}{n} + \max_{\sigma_{AB}} \|\mathcal{E}'(\sigma_{AB}^{\otimes k}) - \mathcal{F}'(\sigma_{AB}^{\otimes k})\|_1.$$

Hence the fixed point properties easily extend to arbitrary inputs via an additive term $O(k/n)$, which vanishes in the limit.

Using Lemma 5 and the previous thoughts we prove Lemma 2 of the main text.

Lemma (Lemma 2 in main text - Product Form Lemma). *Let ρ be an arbitrary mixed state shared by Alice and Bob and let $|\psi\rangle_{ABE}$ be a purification thereof held by Eve. Furthermore, let \mathcal{F} be the ideal protocol and let \mathcal{E} be the real protocol using a distillation protocol satisfying the following properties:*

- (1) *The noise transcripts do not leak to Eve.*
- (2) *The distillation protocol is guaranteed to converge after passing the parameter estimation phase towards a unique and attracting fixed point depending on the noise parameter only.*

Then

$$(\mathcal{E} \otimes id_E)(|\psi\rangle\langle\psi|_{ABE}) - (\mathcal{F} \otimes id_E)(|\psi\rangle\langle\psi|_{ABE})\|_1 \leq (4^7 + 1) \max_{\rho_{AB}} \|\mathcal{E}(\rho_{AB}) - \mathcal{F}(\rho_{AB})\| \quad (47)$$

Proof. The proof relies on Lemma 5. Suppose Eve prepares the pure state $|\psi\rangle_{ABE}$ and let $\text{tr}_E[|\psi\rangle\langle\psi|] = \rho_{AB}$ be the state received by Alice and Bob. Then we have

$$\begin{aligned} (\mathcal{E} \otimes id_E)(|\psi\rangle\langle\psi|) &= p_\rho \sigma_{ABE} \otimes |ok\rangle\langle ok| + (1 - p_\rho) \sigma_{AB}^\perp \otimes \sigma_E \otimes |fail\rangle\langle fail|, \\ (\mathcal{F} \otimes id_E)(|\psi\rangle\langle\psi|) &= p_\rho \sigma_{AB}^\alpha \otimes \sigma_E \otimes |ok\rangle\langle ok| + (1 - p_\rho) \sigma_{AB}^\perp \otimes \sigma_E \otimes |fail\rangle\langle fail|. \end{aligned} \quad (48)$$

If we post-select Eq. (48) on the ok -branch we have after normalization

$$\frac{1}{p_\rho} (id_{ABE} \otimes |ok\rangle\langle ok|) (\mathcal{E} \otimes id_E)(|\psi\rangle\langle\psi|) = \sigma_{ABE} \otimes |ok\rangle\langle ok|. \quad (49)$$

It is obvious from the fact that the protocol is performed by Alice and Bob per definition that any measurement of Eve in the ok -branch can be commuted to the beginning of the protocol \mathcal{E} because Eve is not part of the protocol. Hence her measurement only changes the input of the protocol \mathcal{E} and thus either cause an abort after parameter estimation or not.

We call the final state of Alice and Bob η -Eve-non steerable if for all $\phi \in \mathcal{H}_E$ we have $\|\sigma_{AB}^\phi - \sigma_{AB}\| \leq \eta$ where $\sigma_{AB}^\phi = \text{tr}_E \left[\frac{1}{p_E(\phi)} (id_{AB} \otimes |\phi\rangle\langle\phi|_E) \sigma_{ABE} \right]$. We sketch the remainder of this proof as follows: We show, that the final state of Alice and Bob is Eve-non steerable in the sense of Lemma 5 by making use of the uniqueness of the fixed point of the distillation protocol after passing the parameter estimation phase. Then Lemma 5 completes the proof. More formally, suppose Eve performs a projective measurement on (49) and observes outcome $|\phi\rangle \in \mathcal{H}_E$. Then the post-selected state of Alice, Bob, and Eve conditioned on that particular outcome ϕ reads as

$$\begin{aligned} \frac{1}{p_E(\phi)} (id_{AB} \otimes |\phi\rangle\langle\phi|_E) (\sigma_{ABE} \otimes |ok\rangle\langle ok|) &= \frac{1}{p_E(\phi)} (id_{AB} \otimes |\phi\rangle\langle\phi|_E) \frac{1}{p_\rho} (id_{ABE} \otimes |ok\rangle\langle ok|) (\mathcal{E} \otimes id_E)(|\psi\rangle\langle\psi|_{ABE}) \\ &= \frac{1}{p_\rho} (id_{ABE} \otimes |ok\rangle\langle ok|) (\mathcal{E} \otimes id_E) \underbrace{\left(\frac{id_{AB} \otimes |\phi\rangle\langle\phi|_E}{p'_E(\phi)} |\psi\rangle\langle\psi|_E \right)}_{=:\rho_{ABE}^\phi} = \frac{1}{p_\rho} (id_{ABE} \otimes |ok\rangle\langle ok|) (\mathcal{E} \otimes id_E)(\rho_{ABE}^\phi) \\ &= \sigma_{ABE}^\phi \otimes |ok\rangle\langle ok|. \end{aligned}$$

We note that the state σ_{ABE}^ϕ is in the ok -branch of the real protocol. The next step is to apply Lemma 5 which relates the distances $\|\sigma_{ABE} - \sigma_{AB} \otimes \sigma_E\|$ and $\|\sigma_{AB} - \sigma_{AB}^\phi\|$, i.e. we show that for all $|\phi\rangle \in \mathcal{H}_E$ we have $\|\sigma_{AB} - \sigma_{AB}^\phi\| \leq \frac{2 \max_{\rho_{AB}} \|\mathcal{E}(\rho_{AB}) - \mathcal{F}(\rho_{AB})\|}{p_\rho}$ which then implies using Lemma 5 that $\|\sigma_{ABE} - \sigma_{AB} \otimes \sigma_E\| \leq \frac{4C \max_{\rho_{AB}} \|\mathcal{E}(\rho_{AB}) - \mathcal{F}(\rho_{AB})\|}{p_\rho}$.

First we observe that

$$\begin{aligned} \mathcal{E}(\rho_{AB}) &= p_\rho \sigma_{AB} \otimes |ok\rangle\langle ok| + (1 - p_\rho) \sigma_{AB}^\perp \otimes |fail\rangle\langle fail|, \\ \mathcal{E}(\rho_{AB}^\phi) &= p_\rho \sigma_{AB}^\phi \otimes |ok\rangle\langle ok| + (1 - p_\rho) \sigma_{AB}^\perp \otimes |fail\rangle\langle fail|. \end{aligned}$$

Hence we have

$$\|\mathcal{E}(\rho_{AB}) - \mathcal{F}(\rho_{AB})\| = p_\rho \|\sigma_{AB} - \sigma_{AB}^f\| \quad \text{and} \quad \|\mathcal{E}(\rho_{AB}^\phi) - \mathcal{F}(\rho_{AB}^\phi)\| = p_\rho \|\sigma_{AB}^\phi - \sigma_{AB}^f\|. \quad (50)$$

Using Eq. (50) and the triangle inequality we infer for the distance between σ_{AB} and σ_{AB}^ϕ

$$\|\sigma_{AB} - \sigma_{AB}^\phi\| \leq \|\sigma_{AB} - \sigma_{AB}^\alpha\| + \|\sigma_{AB}^\alpha - \sigma_{AB}^\phi\| \leq \frac{2 \max_{\rho_{AB}} \|\mathcal{E}(\rho_{AB}) - \mathcal{F}(\rho_{AB})\|}{p_\rho}.$$

Thus we apply Lemma 5 to σ_{ABE} with $\epsilon = \frac{2 \max_{\rho_{AB}} \|\mathcal{E}(\rho_{AB}) - \mathcal{F}(\rho_{AB})\|}{p_\rho}$ which implies for the distance between σ_{ABE} and $\sigma_{AB} \otimes \sigma_E$

$$\|\sigma_{ABE} - \sigma_{AB} \otimes \sigma_E\| \leq \frac{4C \max_{\rho_{AB}} \|\mathcal{E}(\rho_{AB}) - \mathcal{F}(\rho_{AB})\|}{p_\rho} \quad (51)$$

where C is a constant depending on the dimensions of the systems of Alice/Bob and Eve. Because the output of Alice and Bob are 2 qubits, the degrees of freedom of Eve after the protocol has finished are also bound by 2 qubits. Hence the constant C is independent of the number of input systems received by Alice and Bob. Finally, employing (51) in (47) yields

$$\begin{aligned} \|(\mathcal{E} \otimes id_E)(|\psi\rangle\langle\psi|) - (\mathcal{F} \otimes id_E)(|\psi\rangle\langle\psi|)\| &= p_\rho \|\sigma_{ABE} - \sigma_{AB}^\alpha \otimes \sigma_E\| \\ &\leq p_\rho (\|\sigma_{ABE} - \sigma_{AB} \otimes \sigma_E\| + \|\sigma_{AB} \otimes \sigma_E - \sigma_{AB}^\alpha \otimes \sigma_E\|) \\ &\leq 4C \max_{\rho_{AB}} \|\mathcal{E}(\rho_{AB}) - \mathcal{F}(\rho_{AB})\| + \max_{\rho_{AB}} \|\mathcal{E}(\rho_{AB}) - \mathcal{F}(\rho_{AB})\| \\ &= (4C + 1) \max_{\rho_{AB}} \|\mathcal{E}(\rho_{AB}) - \mathcal{F}(\rho_{AB})\|. \end{aligned}$$

Before we complete the Lemma we need to determine C . We recall that $C = 4^{n+m} \|T^{-1}\|$ where n and m denote the number of qubits of Alice/Bob and Eve respectively. According to previous thoughts we have $n = m = 2$. Moreover we recall that

$$T = \begin{pmatrix} \langle\phi_1|\sigma_0|\phi_1\rangle\langle\xi_1|\sigma_0|\xi_1\rangle & \dots & \langle\phi_1|\sigma_{4^n}|\phi_1\rangle\langle\xi_1|\sigma_{4^m}|\xi_1\rangle \\ \dots & \dots & \dots \\ \langle\phi_{4^{n+m}}|\sigma_0|\phi_{4^{n+m}}\rangle\langle\xi_{4^{n+m}}|\sigma_0|\xi_{4^{n+m}}\rangle & \dots & \langle\phi_{4^{n+m}}|\sigma_{4^n}|\phi_{4^{n+m}}\rangle\langle\xi_{4^{n+m}}|\sigma_{4^m}|\xi_{4^{n+m}}\rangle \end{pmatrix}$$

We choose $|\phi_{4^3(j_1-1)+4^2(j_2-1)+4(j_3-1)+j_4}\rangle = |\phi'_{j_1}\rangle \otimes |\phi'_{j_2}\rangle \otimes |\phi'_{j_3}\rangle \otimes |\phi'_{j_4}\rangle$ where $j_1, j_2, j_3, j_4 \in 1, 2, 3, 4$ and

$$\begin{aligned} |\phi'_1\rangle &= (|0\rangle + |1\rangle)/\sqrt{2}, \\ |\phi'_2\rangle &= (|0\rangle + i|1\rangle)/\sqrt{2}, \\ |\phi'_3\rangle &= |0\rangle, \\ |\phi'_4\rangle &= (|0\rangle - |1\rangle)/\sqrt{2}. \end{aligned}$$

We observe that the matrix T is invertible and compute using MATLAB $\|T^{-1}\| = 16$. Thus $C = 4^6$ which completes the proof. \square

We emphasize that the previous Lemma does not concern a specific distillation protocol. The proof only requires that the distillation protocol after passing the parameter estimation phase always converges to a *unique* and *attracting* fixed point depending on the noise parameter only. This implies that Lemma 2 of the main text is applicable to the BBPSSW protocol, where we have analytic results regarding its *unique* fixed point, as well as to the DEJMPS protocol, where we have strong numerical evidence regarding its fixed point.

Now we are ready to prove the de-Finetti-based reduction technique as stated in the main text by combining the previous Lemma and Lemma 6 of this supplementary material.

Theorem (de-Finetti-based reduction technique). *Let $\mathcal{E}^{s\&t}$ be the real protocol and $\mathcal{F}^{s\&t}$ the ideal protocol including symmetrization and the tracing out of $n - k$ pairs, taking n input pairs and $k \leq n$. Furthermore we denote by \mathcal{E}' and \mathcal{F}' the remaining sub-protocols after symmetrization and tracing out $n - k$ pairs. Then we have*

$$\max_{|\psi\rangle_{ABE'}} \|(\mathcal{E}^{s\&t} \otimes id_{E'})(|\psi\rangle\langle\psi|) - (\mathcal{F}^{s\&t} \otimes id_{E'})(|\psi\rangle\langle\psi|)\|_1 \leq (4^7 + 1) \left(\frac{64k}{n} + \max_{\sigma_{AB}} \|(\mathcal{E}' - \mathcal{F}')(\sigma_{AB}^{\otimes k})\|_1 \right).$$

Proof. Suppose Eve prepares a purification $|\psi\rangle_{ABE'}$ of the state ρ_{AB} shared by Alice and Bob. Lemma 6 implies that $\|\mathcal{E}^{s\&t}(\rho_{AB}) - \mathcal{F}^{s\&t}(\rho_{AB})\|_1 \leq \frac{64k}{n} + \max_{\sigma_{AB}} \|(\mathcal{E}' - \mathcal{F}')(\sigma_{AB}^{\otimes k})\|_1$. We note that the right hand side of this inequality is independent of ρ_{AB} . Thus Lemma 2 of the main text implies the claim. \square

We point out that the previous theorem is applicable for all noise levels for which distillation is possible.

Reduction for low noise levels via post-selection

As outlined in the main text, we can do better in terms of scaling and efficiency for low noise levels via the post-selection technique [8]. For that purpose we remind the reader that the final state after the distillation protocol including the system of L is pure. Thus, the following Lemma will turn out to be very useful.

Lemma 7. *Let ρ_{AB} and $\varphi_{AB} = |\varphi\rangle\langle\varphi|_A \otimes \mu_B$ be two mixed states. Furthermore, assume that $\rho_A = \text{tr}_B[\rho_{AB}]$ satisfies $\|\rho_A - |\varphi\rangle\langle\varphi|_A\|_1 \leq \varepsilon$ and $\rho_B = \text{tr}_A[\rho_{AB}] = \mu_B$. Then $\|\rho_{AB} - \varphi_{AB}\|_1 \leq 4\sqrt{\varepsilon}$.*

Proof. By assumption we have $\|\rho_A - |\varphi\rangle\langle\varphi|_A\|_1 \leq \varepsilon$. Moreover, let $|\psi\rangle_{ABR}$ be a purification of ρ_{AB} . According to Lemma A.2.7 in [9] there exists a purification $|\varphi\rangle_A \otimes |\xi\rangle_{BR}$ of φ_{AB} such that $\| |\psi\rangle_{ABR} - |\varphi\rangle_A \otimes |\xi\rangle_{BR} \|_{\text{vec}} \leq \sqrt{\|\rho_A - |\varphi\rangle\langle\varphi|_A\|_1} = \sqrt{\varepsilon}$ where $\| |\psi\rangle \|_{\text{vec}} = \sqrt{\langle\psi|\psi\rangle}$ and ${}_{ABR}\langle\psi|\varphi\rangle_A|\xi\rangle_{BR}$ is real and non-negative. Moreover, Lemma A.2.3 of [9] gives

$$\| |\psi\rangle\langle\psi|_{ABR} - |\varphi\rangle\langle\varphi|_A \otimes |\xi\rangle\langle\xi|_{BR} \| \leq 2\| |\psi\rangle_{ABR} - |\varphi\rangle_A \otimes |\xi\rangle_{BR} \|_{\text{vec}} \leq 2\sqrt{\varepsilon}.$$

We define $\xi_B = \text{tr}_R[|\xi\rangle\langle\xi|_{BR}]$. As the 1-norm does not increase under the partial trace we have

$$\|\rho_B - \xi_B\|_1 \leq \|\rho_{AB} - |\varphi\rangle\langle\varphi|_A \otimes \xi_B\|_1 \leq \| |\psi\rangle\langle\psi|_{ABR} - |\varphi\rangle\langle\varphi|_A \otimes |\xi\rangle\langle\xi|_{BR} \|_1 \leq 2\sqrt{\varepsilon}$$

by construction. Moreover, the assumption $\rho_B = \mu_B$ implies $\|\mu_B - \xi_B\|_1 = \|\rho_B - \xi_B\|_1 \leq 2\sqrt{\varepsilon}$. This gives us $\| |\varphi\rangle\langle\varphi|_A \otimes \mu_B - |\varphi\rangle\langle\varphi|_A \otimes \xi_B \|_1 = \|\mu_B - \xi_B\|_1 \leq 2\sqrt{\varepsilon}$. If we combine these results we obtain

$$\|\rho_{AB} - \varphi_{AB}\|_1 = \|\rho_{AB} - |\varphi\rangle\langle\varphi|_A \otimes \mu_B\|_1 \leq \|\rho_{AB} - |\varphi\rangle\langle\varphi|_A \otimes \xi_B\|_1 + \| |\varphi\rangle\langle\varphi|_A \otimes \xi_B - |\varphi\rangle\langle\varphi|_A \otimes \mu_B \|_1 \leq 4\sqrt{\varepsilon}$$

which proves the claim. \square

Lemma 7 enables us to prove Lemma 3 of the main text. For that purpose we first recall the Lemma.

Lemma (Lemma 3 in main text). *Let \mathcal{E} be the real protocol which guarantees to converge towards a unique and attracting fixed point depending on the noise parameter only. Let \mathcal{F} be the ideal protocol as defined in the main text. Furthermore let ρ be a mixed state shared by Alice and Bob. If the extension of \mathcal{E} and \mathcal{F} to the system of L satisfies $\|\mathcal{E}_L(\rho) - \mathcal{F}_L(\rho)\|_1 \leq \varepsilon$, then*

$$(\mathcal{E} \otimes \text{id}_{E'}) (|\psi\rangle\langle\psi|_{ABE'}) - (\mathcal{F} \otimes \text{id}_{E'}) (|\psi\rangle\langle\psi|_{ABE'}) \|_1 \leq 4\sqrt{\varepsilon}$$

for all purifications $|\psi\rangle_{ABE'}$ of ρ .

Proof. As mentioned in the main text, we introduce a two-level flag system held by Alice which indicates whether they aborted the protocol or not. So we observe

$$\begin{aligned} \mathcal{E}_L(\rho) &= p_\rho \sigma_{ABEL} \otimes |ok\rangle\langle ok| + (1 - p_\rho) \sigma_{ABEL}^\perp \otimes |fail\rangle\langle fail|, \\ \mathcal{F}_L(\rho) &= p_\rho |\psi^f\rangle\langle\psi^f|_{ABEL} \otimes |ok\rangle\langle ok| + (1 - p_\rho) \sigma_{ABEL}^\perp \otimes |fail\rangle\langle fail|, \end{aligned}$$

where E denotes the system of leaked noise transcripts to Eve. By assumption we have $\|\mathcal{E}_L(\rho) - \mathcal{F}_L(\rho)\|_1 \leq \varepsilon$. This is equivalent to $p_\rho \|\sigma_{ABEL} - |\psi_f\rangle\langle\psi_f|_{ABEL}\|_1 \leq \varepsilon$ since $\mathcal{E}_L(\rho)$ and $\mathcal{F}_L(\rho)$ are equal on the fail branch. This we can rewrite to $\|\sigma_{ABEL} - |\psi_f\rangle\langle\psi_f|_{ABEL}\|_1 \leq \varepsilon/p_\rho$.

Moreover, applying the real and ideal protocol to the purification $|\psi\rangle_{ABE'}$ results in

$$\begin{aligned} (\mathcal{E} \otimes \text{id}_{E'}) (|\psi\rangle\langle\psi|_{ABE'}) &= p_\rho \sigma_{ABEE'} \otimes |ok\rangle\langle ok| + (1 - p_\rho) \sigma_{ABEE'}^\perp \otimes |fail\rangle\langle fail|, \\ (\mathcal{F} \otimes \text{id}_{E'}) (|\psi\rangle\langle\psi|_{ABE'}) &= p_\rho \sigma_{ABE}^f \otimes \rho_{E'} \otimes |ok\rangle\langle ok| + (1 - p_\rho) \sigma_{ABE}^f \otimes |fail\rangle\langle fail|. \end{aligned}$$

Again, both expression are equal in the fail branch, thus the 1-norm simplifies to

$$\|(\mathcal{E} \otimes \text{id}_{E'}) (|\psi\rangle\langle\psi|_{ABE'}) - (\mathcal{F} \otimes \text{id}_{E'}) (|\psi\rangle\langle\psi|_{ABE'})\|_1 = p_\rho \|\sigma_{ABEE'} - \sigma_{ABE}^f \otimes \rho_{E'}\|_1. \quad (52)$$

Hence it is sufficient to show $p_\rho \|\sigma_{ABEE'} - \sigma_{ABE}^f \otimes \rho_{E'}\|_1 \leq 4\sqrt{\varepsilon}$. We observe that by introducing the system L held by L that

$$p_\rho \|\sigma_{ABEE'} - \sigma_{ABE}^f \otimes \rho_{E'}\|_1 \leq p_\rho \|\sigma_{ABELE'} - |\psi^\alpha\rangle\langle\psi^\alpha|_{ABEL} \otimes \rho_{E'}\|_1. \quad (53)$$

One easily verifies $\text{tr}_{E'}[\sigma_{ABELE'}] = \sigma_{ABEL}$ and $\text{tr}_{ABEL}[\sigma_{ABELE'}] = \rho_{E'}$ because the system E' is not changed by the protocol \mathcal{E} . Moreover, by assumption we have $\|\sigma_{ABEL} - |\psi_f\rangle\langle\psi_f|_{ABEL}\|_1 \leq \varepsilon/p_\rho$. Thus we apply Lemma 7 to $\rho_{A'B'} := \sigma_{ABELE'}$ and $\varphi_{A'B'} = |\psi_f\rangle\langle\psi_f|_{ABEL} \otimes \rho_{E'}$ where $A' := ABEL$ and $B' := E'$ which implies

$$\|\sigma_{ABELE'} - |\psi_f\rangle\langle\psi_f|_{ABEL} \otimes \rho_{E'}\|_1 \leq 4\sqrt{\varepsilon/p_\rho}. \quad (54)$$

Employing (53) and (54) in (52) yields

$$\|(\mathcal{E} \otimes \text{id}_{E'}) (|\psi\rangle\langle\psi|_{ABE'}) - (\mathcal{F} \otimes \text{id}_{E'}) (|\psi\rangle\langle\psi|_{ABE'})\|_1 \leq p_\rho 4\sqrt{\varepsilon/p_\rho} = 4\sqrt{p_\rho \varepsilon} \leq 4\sqrt{\varepsilon}$$

which completes the proof. \square

Moreover, using Lemma 3 of the main text we prove the post-selection-based reduction technique.

Theorem (Post-selection-based reduction technique). *Let \mathcal{E}^s be the real protocol and \mathcal{F}^s the ideal protocol preceded by a symmetrization step operating on n input pairs. Furthermore we denote by \mathcal{E}' and \mathcal{F}' the sub-protocols after symmetrization. Then we have*

$$\max_{|\psi\rangle_{ABE'}} \|(\mathcal{E}^s \otimes id_{E'}) (|\psi\rangle \langle \psi|) - (\mathcal{F}^s \otimes id_{E'}) (|\psi\rangle \langle \psi|)\|_1 \leq 4g_{n,d} \sqrt{\max_{\sigma_{AB}} \|(\mathcal{E}' - \mathcal{F}') (\sigma_{AB}^{\otimes n})\|_1}$$

where $g_{n,d} = \binom{n+15}{n}$.

Proof. We observe that \mathcal{E}^s and \mathcal{F}^s are permutation invariant maps due to the symmetrization step. Thus we can apply the post-selection technique of [8] which implies

$$\max_{|\psi\rangle_{ABE'}} \|(\mathcal{E}^s \otimes id_{E'}) (|\psi\rangle \langle \psi|) - (\mathcal{F}^s \otimes id_{E'}) (|\psi\rangle \langle \psi|)\|_1 \leq g_{n,d} \|(\mathcal{E}^s \otimes id_{E'}) (|\tau\rangle \langle \tau|_{ABE'}) - (\mathcal{F}^s \otimes id_{E'}) (|\tau\rangle \langle \tau|_{ABE'})\|_1 \quad (55)$$

where $|\tau\rangle_{ABE'}$ is a purification of the de-Finetti Hilbert-Schmidt state, hence $\text{tr}_{E'} [|\tau\rangle \langle \tau|_{ABE'}] = \int \sigma_{AB}^{\otimes n} d\mu(\sigma) =: \tau'$ where μ is the measure induced by the Hilbert-Schmidt metric on $\text{End}(\mathbb{C}^4)$. Furthermore, we note that

$$\|\mathcal{E}^s(\tau') - \mathcal{F}^s(\tau')\|_1 = \left\| (\mathcal{E}^s - \mathcal{F}^s) \left(\int \sigma_{AB}^{\otimes n} d\mu(\sigma) \right) \right\|_1 \leq \max_{\sigma_{AB}} \|(\mathcal{E}' - \mathcal{F}') (\sigma_{AB}^{\otimes n})\|_1.$$

As $|\tau\rangle_{ABE'}$ is a purification of τ' we can apply Lemma 3 of the main text which gives, for (55),

$$\max_{|\psi\rangle_{ABE'}} \|(\mathcal{E}^s \otimes id_{E'}) (|\psi\rangle \langle \psi|) - (\mathcal{F}^s \otimes id_{E'}) (|\psi\rangle \langle \psi|)\|_1 \leq 4g_{n,d} \sqrt{\max_{\sigma_{AB}} \|(\mathcal{E}' - \mathcal{F}') (\sigma_{AB}^{\otimes n})\|_1}$$

which completes the proof. \square

Finally, we remind the reader that the preprocessing steps (symmetrization, tracing out) of the distillation protocol and the Lemmas of this section are non-trivial and crucial for the proof of the de-Finetti-based and post-selection-based reduction technique.

Furthermore we point out that the proof regarding the BBPSSW protocol is analytic and necessarily relies on the de-Finetti-based reduction technique because of its slow convergence rate. The rate of convergence for the BBPSSW protocol can easily be derived from (34). For the DEJMPS protocol it turns out that we have polynomial scaling depending on the noise parameter α , i.e. $\max_{\sigma_{AB}} \|(\mathcal{E}' - \mathcal{F}') (\sigma_{AB}^{\otimes n})\|_1 \leq O(n^{b(\alpha)})$.

CONFIDENTIALITY OF ENTANGLEMENT DISTILLATION PROTOCOLS WHENEVER THE NOISE TRANSCRIPTS LEAK

In this section we show how the confidentiality guarantees regarding an entanglement distillation protocol can be extended to the case whenever the noise transcripts leak to Eve.

We remind the reader that it is not necessary to leak the noise transcripts to Eve after every single distillation round. It is sufficient to copy all noise transcripts at the very end to Eve's register, as L is not accessible and Eve is not part of the protocol being executed by Alice and Bob.

Lemma (Lemma 4 in main text). *Let \mathcal{E} be the real protocol and \mathcal{F} be the ideal protocol. Furthermore, let \mathcal{E}^l be the real and \mathcal{F}^l be the ideal protocol when the noise transcripts leak to Eve. Then*

$$\|(\mathcal{E} \otimes id_E) (|\psi\rangle \langle \psi|_{ABE}) - (\mathcal{F} \otimes id_E) (|\psi\rangle \langle \psi|_{ABE})\| \leq \varepsilon$$

implies that

$$\|(\mathcal{E}^l \otimes id_E) (|\psi\rangle \langle \psi|_{ABE}) - (\mathcal{F}^l \otimes id_E) (|\psi\rangle \langle \psi|_{ABE})\| \leq 2\sqrt{\varepsilon}. \quad (56)$$

Proof. We observe that

$$\begin{aligned} (\mathcal{E} \otimes id_E)(|\psi\rangle\langle\psi|) &= p_\rho \sigma_{ABE} \otimes |ok\rangle\langle ok| + (1 - p_\rho) \sigma_{AB}^\perp \otimes \sigma_E \otimes |fail\rangle\langle fail|, \\ (\mathcal{F} \otimes id_E)(|\psi\rangle\langle\psi|) &= p_\rho \sigma_{AB}^\alpha \otimes \sigma_E \otimes |ok\rangle\langle ok| + (1 - p_\rho) \sigma_{AB}^\perp \otimes \sigma_E \otimes |fail\rangle\langle fail|. \end{aligned}$$

So by assumption we have

$$\|(\mathcal{E} \otimes id_E)(|\psi\rangle\langle\psi|) - (\mathcal{F} \otimes id_E)(|\psi\rangle\langle\psi|)\| = p_\rho \|\sigma_{ABE} - \sigma_{AB}^\alpha \otimes \sigma_E\| \leq \varepsilon,$$

i.e. $\|\sigma_{ABE} - \sigma_{AB}^\alpha \otimes \sigma_E\| \leq \varepsilon/p_\rho$.

As outlined in the main text we model L in terms of purifications. Because purifications are unitarily equivalent we choose a particular purification of $\sigma_{AB}^\alpha \otimes \sigma_E$. Thus we fix $|\psi_{\mathcal{F}}\rangle_{ABL_1L_2E} = |\psi'\rangle_{ABL_1} \otimes |\psi''\rangle_{L_2E}$ where $|\psi'\rangle_{ABL_1} = \sum_{i,j} \omega_{ij}(\alpha) |B_{ij}\rangle_{AB} |ij\rangle_{L_1}$. The purifying systems L_1 and L_2 we attribute to the Lab Demon.

Moreover, according to Lemma A.2.7 in [9] there exists a purification $|\psi_{\mathcal{E}}\rangle$ of σ_{ABE} such that $\| |\psi_{\mathcal{F}}\rangle_{ABL_1L_2E} - |\psi_{\mathcal{E}}\rangle_{ABL_1L_2E} \|_{\text{vec}} \leq \sqrt{\varepsilon/p_\rho}$ where $\| |\psi\rangle \|_{\text{vec}} = \sqrt{\langle\psi|\psi\rangle}$ and ${}_{ABL_1L_2E}\langle\psi_{\mathcal{F}}|\psi_{\mathcal{E}}\rangle_{ABL_1L_2E}$ is real and non-negative. Furthermore, Lemma A.2.3 of [9] gives

$$\| |\psi_{\mathcal{E}}\rangle\langle\psi_{\mathcal{E}}|_{ABL_1L_2E} - |\psi_{\mathcal{F}}\rangle\langle\psi_{\mathcal{F}}|_{ABL_1L_2E} \| \leq 2 \| |\psi_{\mathcal{E}}\rangle_{ABL_1L_2E} - |\psi_{\mathcal{F}}\rangle_{ABL_1L_2E} \|_{\text{vec}} \leq 2\sqrt{\varepsilon/p_\rho}. \quad (57)$$

When the noise transcripts leak to Eve, L effectively copies the noise transcripts $|ij\rangle_{L_1}$ to Eve, resulting in the pure state $|\phi\rangle_{ABL_1L_2EE'} = \left(\sum_{i,j} |B_{ij}\rangle_{AB} |ij\rangle_{L_1} |ij\rangle_{E'} \right) \otimes |\psi\rangle_{L_2E}$. Hence we can model the leakage of the noise transcripts to Eve by a unitary U_M such that $U_M |\psi_{\mathcal{F}}\rangle_{ABL_1L_2E} |0\rangle_{E'} = |\phi\rangle_{ABL_1L_2EE'}$. For the protocol when the noise transcripts leak to Eve we have

$$\begin{aligned} (\mathcal{E}^l \otimes id_E)(|\psi\rangle\langle\psi|) &= p_\rho \sigma'_{ABE} \otimes |ok\rangle\langle ok| + (1 - p_\rho) \sigma_{AB}^\perp \otimes \sigma_E \otimes |fail\rangle\langle fail| \\ &= p_\rho \text{tr}_{L_1L_2} \left[U_M |\psi_{\mathcal{E}}\rangle\langle\psi_{\mathcal{E}}| U_M^\dagger \right] \otimes |ok\rangle\langle ok| + (1 - p_\rho) \sigma_{AB}^\perp \otimes \sigma_E \otimes |fail\rangle\langle fail| \\ (\mathcal{F}^l \otimes id_E)(|\psi\rangle\langle\psi|) &= p_\rho \sigma'^\alpha_{ABE} \otimes |ok\rangle\langle ok| + (1 - p_\rho) \sigma_{AB}^\perp \otimes \sigma_E \otimes |fail\rangle\langle fail| \\ &= p_\rho \text{tr}_{L_1L_2} \left[U_M |\psi_{\mathcal{F}}\rangle\langle\psi_{\mathcal{F}}| U_M^\dagger \right] \otimes |ok\rangle\langle ok| + (1 - p_\rho) \sigma_{AB}^\perp \otimes \sigma_E \otimes |fail\rangle\langle fail|. \end{aligned}$$

Because the real and the ideal protocol are equal in the fail-branch we obtain by using (57)

$$\begin{aligned} \|(\mathcal{E}^l \otimes id_E)(|\psi\rangle\langle\psi|_{ABE}) - (\mathcal{F}^l \otimes id_E)(|\psi\rangle\langle\psi|_{ABE})\| &= p_\rho \|\sigma'_{ABE} \otimes |ok\rangle\langle ok| - \sigma'^\alpha_{ABE} \otimes |ok\rangle\langle ok|\| \\ &= p_\rho \left\| \text{tr}_{L_1L_2} \left[U_M |\psi_{\mathcal{E}}\rangle\langle\psi_{\mathcal{E}}| U_M^\dagger \right] - \text{tr}_{L_1L_2} \left[U_M |\psi_{\mathcal{F}}\rangle\langle\psi_{\mathcal{F}}| U_M^\dagger \right] \right\| \\ &\leq p_\rho \left\| U_M |\psi_{\mathcal{E}}\rangle\langle\psi_{\mathcal{E}}| U_M^\dagger - U_M |\psi_{\mathcal{F}}\rangle\langle\psi_{\mathcal{F}}| U_M^\dagger \right\| \\ &= p_\rho \| |\psi_{\mathcal{E}}\rangle\langle\psi_{\mathcal{E}}| - |\psi_{\mathcal{F}}\rangle\langle\psi_{\mathcal{F}}| \| \leq 2\sqrt{\varepsilon p_\rho} \leq 2\sqrt{\varepsilon} \end{aligned}$$

which proves (56). \square

Thus the confidentiality of a protocol where the noise transcripts leak to Eve is bounded by the confidentiality of the same protocol when they do not.

QUANTUM ONE-TIME PADDING AFTER THE REAL PROTOCOL

In this section we show that a final secret twirl applied to the pair of Alice and Bob decouples Eve completely from the remaining state. Keep in mind that for this Alice and Bob require two classical bits unknown to Eve.

Recall that the state of Alice, Bob, Eve, and L after n distillation rounds is pure and of the form $|\psi\rangle = \sum_{i,j,k,l} P_{ijkl} |B_{ij}\rangle_{AB} |\eta_{kl}\rangle_L |\eta_{ijkl}\rangle_E$. Tracing over L yields the mixed state

$$\rho_{ABE} = \sum_{i_1, i_2, j_1, j_2} \sum_{k, l} P_{i_1 j_1 k l} P_{i_2 j_2 k l}^* |B_{i_1 j_1}\rangle\langle B_{i_2 j_2}| \otimes |\eta_{i_1 j_1 k l}\rangle\langle \eta_{i_2 j_2 k l}|. \quad (58)$$

Suppose Alice and Bob apply a secret twirl \mathcal{T} to (58), i.e. they apply stochastically the family of operators $\{id, K_1, K_2, K_1 K_2\}$ where $K_1 = \sigma_x \otimes \sigma_x$ and $K_2 = \sigma_z \otimes \sigma_z$. These are two stabilizers of the Bell state, i.e.,

$$\begin{aligned} K_1^{r_1} |B_{i_1 j_1}\rangle &= (-1)^{i_1 r_1} |B_{i_1 j_1}\rangle, \\ K_2^{r_2} |B_{i_1 j_1}\rangle &= (-1)^{j_1 r_2} |B_{i_1 j_1}\rangle. \end{aligned}$$

Hence, applying the secret twirl \mathcal{T} to (58) gives

$$\begin{aligned} \mathcal{T}\rho_{ABE} &= \sum_{\substack{r_1, r_2 \\ i_1, i_2, j_1, j_2, k, l}} \frac{1}{4} P_{i_1 j_1 k l} P_{i_2 j_2 k l}^* K_1^{r_1} K_2^{r_2} |B_{i_1 j_1}\rangle \langle B_{i_2 j_2}| K_1^{r_1} K_2^{r_2} \otimes |\eta_{i_1 j_1 k l}\rangle \langle \eta_{i_2 j_2 k l}| \\ &= \sum_{\substack{r_1, r_2 \\ i_1, i_2, j_1, j_2, k, l}} (-1)^{i_1 r_1} (-1)^{j_1 r_2} (-1)^{i_2 r_1} (-1)^{j_2 r_2} \frac{1}{4} P_{i_1 j_1 k l} P_{i_2 j_2 k l}^* |B_{i_1 j_1}\rangle \langle B_{i_2 j_2}| \otimes |\eta_{i_1 j_1 k l}\rangle \langle \eta_{i_2 j_2 k l}| \\ &= \sum_{i_1, i_2, j_1, j_2} |B_{i_1 j_1}\rangle \langle B_{i_2 j_2}| \otimes \frac{1}{4} \sum_{k, l} P_{i_1 j_1 k l} P_{i_2 j_2 k l}^* |\eta_{i_1 j_1 k l}\rangle \langle \eta_{i_2 j_2 k l}| \sum_{r_1, r_2} (-1)^{(i_1 + i_2) r_1} (-1)^{(j_1 + j_2) r_2} \\ &= \sum_{i_1, j_1} |B_{i_1 j_1}\rangle \langle B_{i_1 j_1}| \otimes \sum_{k, l} |P_{i_1 j_1 k l}|^2 |\eta_{i_1 j_1 k l}\rangle \langle \eta_{i_1 j_1 k l}|. \end{aligned}$$

Note that in the resulting state $\sum_{i_1, j_1} |B_{i_1 j_1}\rangle \langle B_{i_1 j_1}| \otimes \sum_{k, l} |P_{i_1 j_1 k l}|^2 |\eta_{i_1 j_1 k l}\rangle \langle \eta_{i_1 j_1 k l}|$ Eve decouples, i.e. Alice/Bob and Eve have a separable state. The obtained resource state can be used to establish a perfectly secure quantum channel by means of quantum teleportation.

ROBUSTNESS OF RECURRENCE-TYPE ENTANGLEMENT DISTILLATION PROTOCOL

To complete the security characterization of entanglement distillation protocols we also consider the robustness of an entanglement distillation protocol. To define this term precisely we first need the definition of a honest eavesdropper.

Definition 8. We call an eavesdropper honest, if the states sent by the eavesdropper are of the form $|B_{00}\rangle^{\otimes 2^n}$.

It is obvious that a honest eavesdropper is not entangled with the ensemble delivered to Alice and Bob via the noisy quantum channel. Moreover we formally define the robustness of a protocol by:

Definition 9 (Robustness of a protocol). We call a protocol \mathcal{E}^α ε_R -robust, if for a honest eavesdropper the probability of aborting the protocol is at most ε_R .

Now we show that we can tune the robustness of a recurrence-type entanglement distillation protocol to be exponentially small in terms of necessary number of input pairs.

Theorem 10. Let $M \in \mathbb{N}$ such that Alice and Bob achieve ε -confidentiality by succeeding M rounds of a recurrence-type entanglement distillation. Furthermore assume that Alice and Bob receive n pairs from a honest eavesdropper over the quantum channel $\Phi^{\otimes n}$ (where $\Phi(\rho) = \beta\rho + (1 - \beta)/4 \left(\sum_{i,j} \sigma_{i,j} \rho \sigma_{i,j} \right)$) such that, after the parameter estimation step of the proposed protocol, $k - \sqrt{k}$ pairs (where $k - \sqrt{k} = c2^M$ and $c = \xi 2^{M+2}$) are left for entanglement distillation. Then, the robustness ε_R of the protocol is bounded by

$$\varepsilon_R \leq \exp\left(-(3\beta - 4F_{\min}(\alpha) - 1)^2 \sqrt{k}/128\right) + M \exp(-\xi).$$

Proof. The basic idea of the proof is to request sufficiently many pairs from Eve such that the probabilities of abort during the protocol to be exponentially small while still having enough pairs left to achieve M rounds of a recurrence-type entanglement distillation protocol. We divide the proof into two parts:

- Part 1: We prove that the probability of aborting the recurrence-type entanglement distillation protocol due to parameter estimation is exponentially small.
- Part 2: We prove the same holds true for aborting the protocol during entanglement distillation.

Part 1: Suppose Eve sends the state $|B_{00}\rangle^{\otimes n}$ through the noisy quantum channel $\Phi^{\otimes n}$ to Alice and Bob. Applying Φ to $|B_{00}\rangle\langle B_{00}|$ yields

$$\rho_{AB} = \Phi(|B_{00}\rangle\langle B_{00}|) = (3\beta + 1)/4 |B_{00}\rangle\langle B_{00}| + (1 - \beta)/4 (|B_{10}\rangle\langle B_{10}| + |B_{01}\rangle\langle B_{01}| + |B_{11}\rangle\langle B_{11}|). \quad (59)$$

Thus the state Alice and Bob receive is $\rho_{AB}^{\otimes n}$. According to the preceding protocols proposed in the main text, Alice and Bob apply a symmetrization to $\rho_{AB}^{\otimes n}$, and, depending on the noise of the apparatus, they might have to trace out $n - k$ pairs or not. For the subsequent analysis we assume that this tracing out step is necessary, i.e. the de-Finetti-based reduction needs to be applied. Hence, Alice and Bob continue by applying a twirl to each remaining pair. Since $\rho_{AB}^{\otimes k}$ is invariant under permutations and ρ_{AB} is Bell-diagonal, the remaining state after twirling is equal to $\rho_{AB}^{\otimes k}$.

Next, they apply to \sqrt{k} of the remaining k pairs the parameter estimation for estimating the fidelity of each pair. Necessary for convergence of all recurrence-type protocols is that the fidelity F of ρ_{AB} with $|B_{00}\rangle$ satisfies $F > F_{\min}(\alpha)$. Hence this step is crucial in order to guarantee successful distillation.

For that purpose, we measure $\lfloor \sqrt{k} \rfloor$ of k pairs by applying two-qubit measurements. To be more precise, we apply a $\sigma_x \otimes \sigma_x$ to the first and $\sigma_z \otimes \sigma_z$ measurement to the second pair. We refer to this measurements by M_1 and M_2 respectively. We observe that the state $|B_{00}\rangle$ is a common eigenstate of M_1 and M_2 with eigenvalue 1. We define to each pair of pairs a random variable X_i for $i \in \{1, \dots, \lfloor \sqrt{k} \rfloor / 2\}$ with $X_i = 1$ whenever both measurements M_1 and M_2 yield outcome 1 and $X_i = 0$ else.

Furthermore we assume for the expected value $\mathbb{E}(X)$ of the fidelity with $|B_{00}\rangle$ that $\mathbb{E}(X) = F_{\min}(\alpha) + \delta$, where $\delta > 0$ will be fixed below. The protocol will be aborted if the estimate is below $F_{\min}(\alpha) + \delta$.

From (59) we observe that, whenever $(3\beta + 1)/4 \leq F_{\min}(\alpha)$, the entanglement distillation protocol will not distill any entanglement. This implies for the quantum channel Φ that, if $\beta \leq (4F_{\min}(\alpha) - 1)/3$ the parameter estimation step will abort, independent of the input provided by Eve. Thus we assume for the subsequent analysis that $\beta > (4F_{\min}(\alpha) - 1)/3$.

Moreover we define $\eta = \delta/2$. Hence we get by the Hoeffdings inequality for the probability of an error larger than η in our measured estimate \bar{X} for the fidelity the following expression:

$$\mathbb{P}(|\mathbb{E}(X) - \bar{X}| \geq \eta) \leq \exp(-\eta^2 \sqrt{k}/2) =: p_{\text{pe-abort}}.$$

Thus the probability of aborting the protocol due to an error in the parameter estimation is exponentially small in number of necessary input pairs. In order to fix δ we recognize that Alice and Bob abort the protocol whenever $(3\beta + 1)/4 < F_{\min}(\alpha) + \delta$. This is equivalent to $\delta > (3\beta - 4F_{\min}(\alpha) - 1)/4$. Inserting the definition of η yields $\eta > (3\beta - 4F_{\min}(\alpha) - 1)/8$ and thus $p_{\text{pe-abort}} < \exp(-(3\beta - 4F_{\min}(\alpha) - 1)^2 \sqrt{k}/128)$.

Part 2: What remains to be shown is that the probability of aborting the protocol in the distillation phase is also exponentially small in the number of input pairs. For that purpose, we assume that the noise level α of the apparatus is such that distillation is feasible. In the following we show that we can force the probability of abort due to entanglement distillation to be exponentially small in terms of requested input pairs.

We assume that Alice and Bob are left with $c2^M$ pairs after parameter estimation. Recall that the Chernoff inequality for a sequence of independent Bernoulli random variables X_1, \dots, X_n where $\mathbb{P}(X_i = 1) = p$ and $d \in [0, 1]$ reads as

$$\mathbb{P}\left(\sum_i X_i \leq (1 - d)pn\right) \leq \exp\left(-\frac{d^2}{2}pn\right).$$

Moreover, we observe that a basic distillation step can be modelled by a Bernoulli random variable X_i where $\mathbb{P}(X_i = 1) = p$ is the probability of succeeding (measurement outcomes coincide).

Suppose we perform m rounds of entanglement distillation. Let N_m denote the number of input pairs to the m -th round and let $d \in [0, 1]$. Then the Chernoff inequality implies that the probability that less than $(1 - d)pN_m$ basic distillation steps at round m have succeeded is bounded by $\exp(-\frac{d^2}{2}pN_m)$, i.e.

$$p_{\text{abort},m} = \mathbb{P}\left(\sum_i X_i \leq (1 - d)pN_m\right) \leq \exp\left(-\frac{d^2}{2}pN_m\right). \quad (60)$$

But this also implies that, with probability $1 - p_{\text{abort},m}$, at least $(1 - d)pN_m + 1$ basic distillation steps have succeeded at round m . Thus we may safely assume that $N_{m+1} = (1 - d)pN_m + 1$. Furthermore we have $N_1 = c2^M$. Eliminating

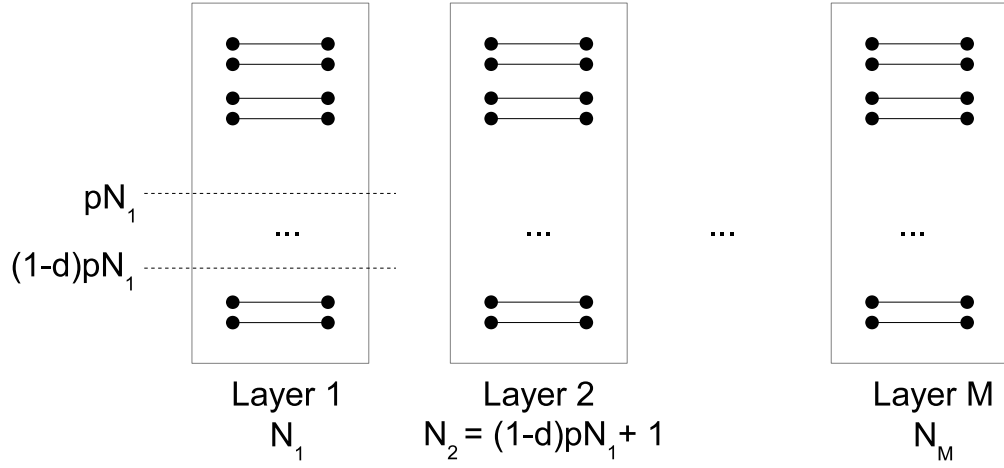


FIG. 8. M rounds of entanglement distillation

the recurrence relation yields $N_{m+1} = (1-d)^m p^m c 2^M + \sum_{i=0}^{m-1} (1-d)^i p^i$. This implies for (60)

$$p_{\text{abort},m} \leq \exp \left(-\frac{d^2}{2} p \left((1-d)^{m-1} p^{m-1} c 2^M + \underbrace{\sum_{i=0}^{m-2} (1-d)^i p^i}_{>0} \right) \right) \leq \exp \left(-\frac{d^2}{2} (1-d)^{m-1} p^m c 2^M \right).$$

Furthermore, we compute the probability of aborting the protocol at distillation round m (assuming that the previous rounds $1, \dots, m-1$ succeeded) by

$$p_{\text{abort at round } m} = p_{\text{abort},m} \underbrace{\prod_{k=1}^{m-1} p_{\text{succeed},k}}_{\leq 1} \leq p_{\text{abort},m} \leq \exp \left(-\frac{d^2}{2} (1-d)^{m-1} p^m c 2^M \right). \quad (61)$$

The events of aborting the distillation protocol at two different rounds i and j are disjoint. Thus we have for the probability of aborting in any of m rounds $p_{\text{abort in any of } m \text{ rounds}} = \sum_{k=1}^m p_{\text{abort at round } k}$. A simple consequence thereof is

$$p_{\text{abort in any of } M \text{ rounds}} = \sum_{k=1}^M p_{\text{abort at round } k} \leq \sum_{k=1}^M \exp \left(-\frac{d^2}{2} (1-d)^{k-1} p^k c 2^M \right) \quad (62)$$

where we have used (61). Inserting $p = 1/2$ and $d = 1/2$ in (62) yields

$$\begin{aligned} p_{\text{abort in any of } M \text{ rounds}} &\leq \sum_{k=1}^M \exp \left(-\frac{1}{8} \frac{1}{2^{2k-1}} c 2^M \right) = \sum_{k=1}^M \exp \left(-c 2^{M-2k-2} \right) \leq M \exp \left(-c 2^{M-2M-2} \right) \\ &= M \exp \left(-c 2^{-(M+2)} \right). \end{aligned} \quad (63)$$

By assumption we have $c = 2^{M+2} \xi$ which implies for (63)

$$p_{\text{abort in any of } M \text{ rounds}} \leq M \exp \left(-\xi 2^{M+2} 2^{-(M+2)} \right) = M \exp \left(-\xi \right).$$

Thus, the probability of aborting the protocol satisfies

$$\varepsilon_R \leq p_{\text{pe-abort}} + (1 - p_{\text{pe-abort}}) p_{\text{abort in any of } M \text{ rounds}} \leq \exp \left(-(3\beta - 4F_{\min}(\alpha) - 1)^2 \sqrt{k}/128 \right) + M \exp \left(-\xi \right)$$

which completes the proof. \square

ESTABLISHING A SECURE QUANTUM CHANNEL

For illustration purposes, we show how private quantum channels can be realized using our proposal in conjunction with standard teleportation. By our results, the joint state of Alice, Bob, and Eve after the distillation protocol is ϵ close to the output of the ideal protocol. The latter, since the register of L is not accessible to any of the parties and thus is traced out, yields the state of the form (provided the protocol was not aborted)

$$\rho_{final} = \sum_{i,j} |\omega_{ij}(\alpha)|^2 |B_{ij}\rangle \langle B_{ij}|_{AB} \otimes |\eta_{ij}\rangle \langle \eta_{ij}|_E. \quad (64)$$

The teleportation of any state ρ from Alice to Bob will yield the state

$$\sum_{i,j} |\omega_{i,j}(\alpha)|^2 \sigma_x^j \sigma_z^i \rho \sigma_z^i \sigma_x^j \otimes |\eta_{ij}\rangle \langle \eta_{ij}|_E. \quad (65)$$

Thus the only information Eve can obtain is what noise operator was applied on the teleported state, and nothing more – thus, the channel is private. Moreover, the probabilities for the different noise processes are not under Eve's control, but depend on the local devices.